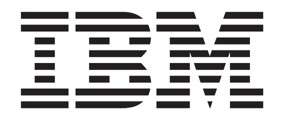
IBM Tealeaf Application de capture passive CX
Version 3650 and 3700
12 juin 2014

Manuel PCA



Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 297.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.can.ibm.com (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

Cette édition s'applique à la génération 3650 et 3700 d'IBM Tealeaf Application de capture passive CX et à toutes les éditions et modifications ultérieures, sauf indications contraires dans les nouvelles éditions.

Table des matières

Avis aux lecteurs canadiens ix

Manuel de l'application Passive Capture xi

Chapitre 1. Présentation de Passive Capture 1

Enhanced International Character Support (EICS) pour Application de capture passive CX version 3700. 1
Sécurité et Administration 1
Prise en charge du protocole SSL 2
Intégration avec les HSM 2
Architecture de déploiement 2
Capacité de traitement de la PCA 5
Présentation de Packet Forwarder 6
Architecture du logiciel 6
Processus de capture. 7
Captured 7
Listend 7
Reassd 7
Pipelined 7
Routerd 7
Tcld 8
Deliverd 8
Failoverd 8
Memcached. 8
Présentation de l'équilibrage de charge transparent de d'CX PCA 8
Instances multiples 9
Processus de pipeline à plusieurs instances . . . 9
Cartes d'un pipeline à plusieurs instances . . . 10
Programme de maintenance 10
Console Web 10
Logiciel tiers 10
Commandes de ce manuel 11
Besoins du trafic de capture du réseau Tealeaf PCA 11
Conditions de base nécessaires au trafic 12
Chiffrement Diffie-Hellman 12
Extension de tickets de session TLS 13
Connexions TCP. 13
Données dupliquées 13
Origine des anomalies relatives à la qualité du trafic réseau 14
Paquets réseau TCP abandonnés 14
Trafic unidirectionnel 14
Evaluation du nombre de paquets abandonnés . . 15

Chapitre 2. Installation 17

Liste de vérification de préinstallation 17
Configuration du trafic réseau 17
Configuration matérielle 18
Cartes accélératrices prises en charge 18
Configuration du système d'exploitation. . . . 19
Recommandations de partitions pour le disque dur 22
Instances multiples de la PCA 22
Modifications effectuées sur le serveur de la PCA 24
Installation des packs 25
Copie du pack d'installation à partir du CD-ROM 25
Installation du RPM tealeaf-pca. 25
Exécution de la PCA pour la première fois en tant qu'utilisateur racine 26
Installation du produit Packet Forwarder . . . 26
Liste de contrôle après installation. 29
Vérification de l'installation de la PCA 29
Création de clés SSL 29
Démarrage de la PCA 30
Configuration initiale de la PCA 30
Vérification des paramètres de connexion autorisée 30
Configuration de la PCA pour la capture d'applications Internet riches 31
Service Tealeaf Passive Capture. 32
Correctifs CX PCA 33
Traitement des incidents et conseils 33
Fichiers CORE 33
Retards au démarrage 33
Remarques relatives à la mise à niveau de la PCA 34
Avant la mise à niveau 35
Mise à niveau basique 36
Mise à niveau de la PCA avec une authentification d'utilisateur 36
Configuration de nouveaux types de données . . 37
Désinstallation ou annulation du logiciel Application de capture passive CX 38
Désinstallation du logiciel Packet Forwarder . . . 39

Chapitre 3. Configuration de CX PCA 41

Présentation de la configuration de Passive Capture 41
Configuration à l'aide de la console Web 41
Configuration à l'aide de `ctc-conf.xml` 41
Configuration à l'aide de `runtime.conf` 41
Fichiers. 42
Enregistrement des modifications 42
Déchiffrement SSL 42
A. IU Web : 42
B. Ligne de commande : 42
C. Redémarrage des services : 42
Référence de la ligne de commande de la PCA Tealeaf 43
Configuration initiale de la PCA 45
Prérequis 46
Exemple de configuration 46
Situations complexes 46
Etapes de configuration 47
Apache : démarrage 47
Ouverture de la console Web de la PCA 47
Configuration de l'interface CX PCA 48
Configuration de la distribution des hits. . . . 50
Configuration du pipeline de la PCA 51
Configuration de la confidentialité. 52

Activation de la capture 53
Test de votre configuration 53
Navigateurs pris en charge pour la console Web de la PCA 54
Connexion à la console Web de la PCA 54
Déconnexion de la console Web de la PCA 55
Onglets de la console Web 55
Configuration 56
Activation de l'authentification pour la console Web 56
Changement d'accès HTTP/HTTPS 56
Déploiement d'un certificat SSL pour la console Web 57
Modification des ports d'écoute de la console Web 57
Prise en charge du format IPv6 dans la console Web de la PCA 57
Page InfoSys 58
Système 58
dmesg 59
Console Web de la PCA - Onglet Récapitulatif . . 60
Statistiques des composés de l'instance 60
Le pourcentage de paquets étrangers 61
Si true, reassd ne peut pas suivre listend . . . 62
Pourcentage de connexions dont les paquets ont été abandonnés 62
Pourcentage de trafic unidirectionnel 62
Le débit reassd rassemble actuellement des hits non-SSL 62
Si true, protocole Diffie-Hellman pour le chiffrement SSL rencontré 63
Pourcentage d'anciennes connexions 63
Clés SSL par seconde manquantes 64
Trafic de kilooctets par seconde filtré 64
Abandon des hits en raison d'une surcharge du processus pipelined lorsque la valeur est différente zéro. 64
Abandon des paquets lorsqu'ils dépassent la taille maximale autorisée quand la valeur est différente de zéro. 65
Connexions TCP. 66
Santé de la machine 67
Statistiques de montage 67
Homologues 68
Statistiques Current Per Second. 68
Informations de débogage supplémentaires de la console Web de la PCA 69
Console Web de la PCA - Onglet Console . . . 70
Console Web de la PCA - Onglet Interface . . . 71
Affichage des instances 73
Désactivation de la validation de total de contrôle des paquets 74
Segmentation du trafic. 74
Filtrage des adresses IP et de port de l'hôte du serveur Web 75
Filtrage de la segmentation du port TCP client . 76
Renseignement des ports 76
Règles de filtrage 78
Liste des instances 83
Trafic à ignorer 85
Modification des filtres 86
Format CIDR 87
Trafic du miroir de port 87
Paramètres d'optimisation 88
Modification manuelle de la configuration de l'interface 90
Filtres VLAN 91
Console Web de la PCA - Onglet Distribution . . 92
Destinataires cible 92
Nombre maximum de destinataires 93
Exemple : ajouter un destinataire 94
Paramètres d'optimisation 94
Utilisation du service de transport Tealeaf comme horloge de référence 95
Distribution de statistiques au service de transport Tealeaf 96
Console Web de la PCA - Onglet Clés SSL . . . 97
Clés chargées 97
Modification d'une clé privée 99
Ajout d'une clé privée 99
Clés manquantes 99
Clés de capture. 101
Génération de vos propres certificats SSL 101
Console Web de la PCA - Onglet Pipeline . . . 101
Paramètres du pipeline 102
Instances du pipeline. 102
Mise en sessions des données 104
X-Forwarding 104
Echantillonnage de session 106
Mode de capture 106
Méthodes de demande de capture 107
Niveau de temps 107
Traitement des hits 107
Listes des types de capture 112
Mode d'évaluation de la PCA pour les types de capture 114
Types de contenu capturés par défaut 115
Extensions de fichier exclues 116
Extensions de fichier autorisées 116
Capturer tous les types Mime 116
Capture de la totalité des types de POST . . . 116
Types de POST XML 116
Types de POST binaires 117
Capture de la totalité des types de codage de contenu 117
Types de contenu et indexation 118
Téléchargement de la configuration de confidentialité 118
Manipulation des règles 118
Manipulation des tests 119
Manipulation de l'action. 119
Manipulation des clés 119
Ajout/modification de règles 120
Ajout/modification de tests 122
Ajouter/modifier des actions 124
Ajout/modification de clés 128
Références du fichier `Privacy.cfg` 129
Règles 130
Tests 131
Actions 131
Consignation des modifications 136
Modifications de la confidentialité 136

Consignation des différences 136
Référence. 136
Statistiques par instance 137
Vérification de l'intégrité du système à l'aide de `stats.xml` 137
Processus du logiciel de capture 138
Statistiques de Passive Capture 138
Section Général. 138
Section Temps 139
Section Mémoire 140
Section TCP 143
Section SSL 145
Section Hits 149
Section Capture 156
Section Destinataires cible 157
Section Reprise 158
Console Web de la PCA - Onglet Journaux de sauvegarde 159
Console Web de la PCA - Onglet Reprise . . . 161
Pulsations 162
Paramètres automatiques 162
Contrôleurs à distance 163
Console Web de la PCA - Onglet Utilitaires . . 163
Interfaces réseau 163
Page Détails 164
bwMon 165
Utilitaires du système 166
Console Web de la PCA - Page Débogage . . . 168
Accès à la page Débogage 168
Page Présentation 168
Sortie de débogage 169
Fichier ZIP de la PCA pour bénéficier du support 170
Contenu du fichier ZIP 170
Fichier de configuration Passive Capture `ctc-conf.xml` 171

Chapitre 4. Configuration de Packet Forwarder 189
Configuration d'un Packet Forwarder pour communiquer avec le logiciel CX PCA 189
Configuration d'un destinataire Packet Forwarder et du logiciel CX PCA pour recevoir des paquets transférés. 191

Chapitre 5. Clés SSL 193
Paramétrage des clés SSL chiffrées 193
Présentation 193
Conversion automatique des clés SSL 194
Conversion automatique des fichiers PEM en fichiers PTL sur le serveur de la PCA 194
Conversion d'une clé privée SSL au format PFX en PTL 194
Etapes pour convertir les clés SSL manuellement 195
Chargement de la PCA avec des clés SSL . . . 195
Fichiers PTL chargés automatiquement 197
Exportation la clé privée SSL 198
Microsoft IIS 5 et 6 199
Microsoft IIS 3.0 et 4.0 200
SunOne (iPlanet) 6.0 200
Traitement des anomalies d'iPlanet 6.0 201
Sun iPlanet 4.x 203
Apache 1.3.x, 2.0.x. 204
IBM HTTP Server 205
Exportation à partir d'un magasin de clés Java (JKS) 205
Solution de contournement de l'outil de clé de Java 206
Création d'un certificat autosigné. 207
Création du certificat autosigné à l'aide de l'algorithme SHA-2 208
Création d'une demande de certificat signé adressée à l'autorité de certificat interne 208
Scripts utilitaires 209
Déploiement des certificats SSL utilisables par la console Web de la PCA 210
Configuration du service de transport Tealeaf pour le chiffrement SSL 210
Test du certificat SSL utilisé par le service de transport 212
Activation des statistiques PCA dans le statut de Tealeaf 213
Suppression ou consultation du certificat 213
Validation des clés PEM 213

Chapitre 6. Mesure des performances 215
Présentation de l'horodatage 215
Hypothèses 215
Exemples d'horodatages dans la demande. . . . 216
Définitions et valeurs d'horodatage dans la demande 216
Calcul de durées à partir des horodatages . . . 218
Facteurs ayant des répercussions sur les valeurs d'horodatage 219
Horodatages dans les hits ReqCancelled . . . 219
Hits sans horodatage 220
Notification des horodatages dans le portail et dans RTV. 221
Durée de création d'une page 221
Durée réseau 221
Durée de l'aller-retour 222
Durée de rendu 222
Test du traitement des performances par Tealeaf 222
Génération de rapports 223
Références 223

Chapitre 7. Configuration de Passive Capture sur Red Hat Enterprise Linux (RHEL) 225
Passive Capture sur RHEL - Configuration du DNS 225
/etc/nsswitch.conf 225
Désactivation du DNS 225
Activation du DNS 225
/etc/resolv.conf 226
Passive Capture sur RHEL - Configuration des interfaces réseau 226
Exemple DHCP 226
Exemple ETHTOOL_OPTS 226
Exemple d'interface d'écoute 227
Exemple d'adresse IP statique 228
Lecture complémentaire 229

Passive Capture sur RHEL - Configuration du NTP 229
Installation du pack NTP 229
Sélection des serveurs NTP 229
Création des fichiers de configuration 230
Activation et démarrage du service 230
Passive Capture sur RHEL - Configuration de l'accès au port série 230

Chapitre 8. Surveillance de Passive Capture 231

Liste de contrôle pour le diagnostic des anomalies de la PCA 231
Liste de contrôle principale 231
Liste de contrôle de configurations supplémentaires de la PCA 232
Conseils supplémentaires pour le diagnostic des anomalies 232
Surveillance de Passive Capture via le statut de Tealeaf 233
Consignation pour l'application Passive Capture 233
Journaux de la PCA 234
Journaux du serveur Apache 234

Chapitre 9. Configuration matérielle et installation du système d'exploitation . 235

Configuration matérielle 235
Etapes de la préinstallation 235
Configuration générale 236
Désactivation des iptables 236
Hyper-Threading 236
Installation de Red Hat Enterprise Linux 236
Désactivation de SELinux 236
RHEL5 237
Sécurité de la console Web 237
Désactivation du serveur Web pour la console Web 237
Désactivation de l'accès à la console Web à partir du port 8080 238
Activation de l'accès à la console Web via une seule adresse IP 238
Application de l'authentification pendant l'accès à la console Web 238
Application immédiate des modifications apportées à la configuration 239
Utilisateurs des systèmes d'exploitation. 239
Mises à niveau du système d'exploitation 240

Chapitre 10. Maintenance de Passive Capture 241

Présentation 241
Diagnostic d'intégrité de la capture 241
Redémarrage de la capture 241
Emplacement des fichiers journaux 241
Consignation des statistiques 242
Synchronisation horaire 242
Configuration manuelle 243

Annexe A. Annexes PCA 247

Annexe B. Annexe - Cartes accélératrices prises en charge . . . 249

Cartes accélératrices prises en charge 249

Annexe C. Système de gestion des clés nCipher SSL. 251

Remarques relatives à nCipher 251
Comatibilité d'IBM Tealeaf CX PCA et de nCipher 252
Installation de nCipher 252

Annexe D. Annexe - Intégration des clés SSL de Tealeaf avec HSM 253

Intégration avec le HSM de nCipher. 253
Hypothèses 253
Exigences. 253
Configuration de PCA 254
Configuration et intégration du HSM 254
Intégration 254
Désactivation du HSM 255
Instructions d'installation 255
Installation du HSM de nCipher pour la PCA . . 255
Conditions préalables 255
Prérequis 256
Etapes d'installation et de création de nCipher . . 256
Création d'un pilote de noyau 256
Installation du pilote du noyau nCipher . . . 257
Confirmation que le logiciel est installé. . . . 258
Installation du logiciel PCA 259
Configuration des scripts de démarrage de nCipher pour un démarrage avant la PCA . . 259
Création d'un environnement sécurisé nCipher pour la PCA. 261
Validation de l'environnement sécurisé 262
Importation des clés SSL dans le magasin de clés nCipher 263
Contrôle de l'utilisation des clés privées SSL . . 264
Désactivation du lancement de nCipher lors du démarrage de Passive Capture 264

Annexe E. Annexe - Rubriques Passive Capture supplémentaires . . 265

Système d'exploitation 265
Installation 265
Configuration du serveur Web. 265
Configuration de la PCA 265
Console 265
Journaux 265
Autre 266
Traitement des incidents. 266
Passive Capture prend-il en charge la version 64 bits de Linux ? 266
Passive Capture prend-il en charge FreeBSD . . . 266
Comment rendre l'installation et la configuration de la PCA automatiques ? 267
De quels packs le RPM tealeaf-pca a-t-il besoin ? 267
Quelles modifications le RPM tealeaf-pca effectue-t-il sur le serveur de la PCA ? 268

Comment définir le répertoire pour le lien symbolique de tealeaf ? 270
Comment désactiver la création d'un lien symbolique tealeaf ? 270
Comment effectuer l'installation dans un autre répertoire que celui défini par défaut ?. 270
Quels répertoires et quels fichiers ne se situent pas dans le répertoire d'installation ? 271
Comment retirer le système de chiffrement Diffie-Hellman de la liste des chiffrements SSL de serveur Web ? 273
Choix de l'emplacement des serveurs à l'aide du système Diffie-Hellman 273
Désactivation 274
  Désactivation du système de chiffrement Diffie-Hellman sur des serveurs IIS 274
  Désactivation du système de chiffrement Diffie-Hellman sur des serveurs Apache . . . 274
Certains hits SSL n'apparaissent pas dans les sessions de navigation de Firefox 275
Symptômes 275
A tester 276
A réparer 276
  Navigateur Firefox 276
  Proxy Web 277
  Serveurs Web Apache 277
  Serveurs Web autres que les serveurs Apache 277
Comment définir d'autres fichiers de configuration ? 277
  Question 277
  Réponse 277
Pourquoi la console Web de la PCA ignore-t-elle les modifications que j'ai enregistrées ? 279
Pourquoi est-il impossible d'interrompre les processus de la console Web ? 279
Où se trouve le répertoire de journaux ctccap ? . . 280
Comment modifier le répertoire de fichiers journaux manuellement ? 280
  Question 280
  Réponse 280
Comment faire pour que la PCA efface automatiquement ses statistiques ? 281
Quel est le numéro de port par défaut correspondant au basculement ? 282
Comment la PCA gère-t-elle la duplication des paquets TCP ? 282
Comment la PCA identifie-t-elle les pages ReqCanceled ? 283
Valeurs côté serveur 283
Valeurs calculées par la PCA 283
Analyse des valeurs de taille du contenu 284
Codage de transfert en blocs 284
Identification des hits ReqCancelled dans Tealeaf 285
  Données enregistrées 285
  Création d'un événement 285
  Recherche de sessions avec ReqCancelled Type 287
Comment la PCA gère-t-elle la capture des adresses IPv6 ? 289
Présentation d'IPv6 289
  Format IPv4 290
  Format IPv6 290
Activation de la capture d'adresses IPv6 291
Capture 292
  Méthodes de capture et de conversion d'adresses IP 292
  Prise en charge du protocole IPv6 par la PCA 292

Annexe F. Documentation et aide d'IBM Tealeaf 295

Remarques 297
Marques 299
Remarques sur les règles de confidentialité . . . 299

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :
- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
⇖ (Pos1)	⇖	Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

Manuel de l'application Passive Capture

Le manuel d'IBM Tealeaf Application de capture passive CX explique en détail comment configurer et utiliser IBM Tealeaf Application de capture passive CX. Ce logiciel capture toutes les demandes et réponses d'une application Web et les assemble pour que le système Tealeaf puisse les utiliser. Utilisez les liens suivants pour accéder à des rubriques précises du manuel.

Chapitre 1. Présentation de Passive Capture

Passive Capture de Tealeaf capture et enregistre toutes les interactions entre le visiteur et l'environnement de l'application Web à l'aide d'un TAP réseau ou d'un port de surveillance de commutateur réseau. Le logiciel Passive Capture offre les fonctionnalités suivantes :

- Le serveur Web ne connaît aucun frais supplémentaire, aucun délai d'attente et il n'utilise pas le processeur
- L'application Web ne connaît aucun risque de panne : le trafic contrôlé/capturé ne fait pas partie du trafic actif
- Il prend en charge tout type d'environnement d'application Web : homogène ou mixte, en pack ou encore personnalisé
- Il prend en charge les trafics chiffré (HTTPS) et non chiffré (HTTP)
- Prend en charge le déploiement dans l'Amazon Web Services (AWS) cloud basé sur l'environnement
- Il reconstruit le trafic HTTP de l'utilisateur pour un traitement en aval des sessions et événements utilisateur

Pour capturer des demandes et des réponses du trafic de votre site Internet, IBM Tealeaf Application de capture passive CX a besoin d'une source de données de très bonne qualité fournie par un réseau fiable. Voir «Besoins du trafic de capture du réseau Tealeaf PCA», à la page 11.

Enhanced International Character Support (EICS) pour Application de capture passive CX version 3700

IBM Tealeaf Application de capture passive CX version 3700 prend en charge la capture de données qui est codée à l'aide d'EICS. Application de capture passive CX version 3700 est utilisé pour capturer le trafic Web pour le traitement par IBM Tealeaf CX version 9,0A.

IBM Tealeaf version 9.0A offre les mêmes fonctionnalités que la version 9.0, mais inclut également les fonctionnalités supplémentaires suivantes :

- Prise en charge de tous les codages Web courants, y compris ceux communément utilisés pour les pages Web codées en japonais, chinois et coréen.
- Meilleurs codage, recherche, filtrage et classement sur les données non ASCII (caractères autres que A-Z, a-z, 0-9, et ponctuation courante).
- Prise en charge lorsque les données utilisateur traitées sont différentes du codage de caractères natifs du système d'exploitation. Par exemple, les composants Tealeaf peuvent traiter des données arabes sur un système d'exploitation Windows français.

Sécurité et Administration

Le logiciel Tealeaf Passive Capture est hautement contrôlé et sécurisé. Il est lié au poste de travail hôte du processus de capture et peut fonctionner sans interface publique. Toutes les fonctions d'administration peuvent être gérées par un programme client Secure Shell (SSH).

- Une interface de console Web sécurisée est disponible pour les fonctions d'administration et de gestion.

Prise en charge du protocole SSL

Le logiciel Tealeaf Passive Capture offre une prise en charge complète des transactions SSL (HTTPS).

Remarque : Pour prendre en charge le SSL, il est nécessaire de fournir une copie des clés privées SSL au logiciel Tealeaf Passive Capture. Si plusieurs certificats SSL existent, une copie de chaque clé privée est nécessaire. Ceci permet à Passive Capture de déchiffrer le trafic SSL pour le traitement du contenu des hits HTTP.

Intégration avec les HSM

Dans certains environnements, les restrictions de sécurité à l'échelle du système d'exploitation sont insuffisantes pour la gestion des clés privées chiffrées. Dans ces environnements, Tealeaf prend en charge les intégrations à l'aide de modules de sécurité matérielle. Un module de sécurité matérielle (HSM) fournit à la fois une protection logique et physique des clés SSL privées sensibles contre les utilisations non-autorisées et les ennemis potentiels.

Alors que l'importation et l'exportation des clés privées SSL vers le serveur d'IBM Tealeaf Application de capture passive CX à l'aide des HSM ne s'effectue pas de la même manière d'un environnement à l'autre, ces transferts ont pour but de stocker les clés de façon sécurisée sur le HSM. Les fournisseurs de HSM offrent des solutions qui répondent aux besoins de ce processus de transfert et comprennent en général plusieurs méthodes compatibles d'installation des clés sur les HSM. Elles comprennent aussi la plupart du temps des aspects de la conception du processus d'installation automatique spécifiques à sa mise en oeuvre.

Dans un environnement HSM, les clés utilisées par Tealeaf lorsque ce logiciel est en cours d'exécution obtiennent les mesures protectrices offertes par le HSM. Le fichier de clés est stocké sur le HSM et conserve un contrôle d'accès renforcé qui prévient tout mouvement.

- Pour plus d'informations sur l'intégration avec un HSM, voir Annexe D, «Annexe - Intégration des clés SSL de Tealeaf avec HSM», à la page 253.
- Sans HSM, les clés privées SSL sont converties en fichier chiffré Tealeaf.ptl et stockées dans un répertoire du système d'exploitation sous une forme utilisable sur le même poste de travail uniquement ; la clé est hachée d'une manière propre à la machine. Pour plus d'informations sur cette méthode, voir «Paramétrage des clés SSL chiffrées», à la page 193.

Architecture de déploiement

Passive Capture se compose d'un logiciel qu is'exécute sur un hôte, qui se connecte directement au dispositif de collecte, un tap network ou un port d'étalement de commutateur. Le flux de données qui circule du dispositif de collecte au poste de travail hôte ne se fait que dans une direction : l'hôte ne fait que recevoir les données de façon passive.

Passive Capture transporte les données depuis l'hôte vers l'environnement du serveur d'IBM Tealeaf CX en temps réel. Les données peuvent être transportées par le protocole TCP/IP ou par le biais d'un câble croisé qui relie directement l'hôte de Passive Capture au poste de travail qui reçoit les données dans l'environnement d'IBM Tealeaf CX. Passive Capture effectue les fonctions suivantes :

- Reconstruction des corps de demande et de réponse HTTP(S) à partir des données du paquet TCP/IP capturé

- Déchiffrement du SSL (si applicable)
- (facultatif) Mise en session (ou en séquence) des pages de demande et de réponse HTTP par un ID session dans les sessions visiteur
- (facultatif) Possibilité de configuration de paramètres de confidentialité permettant de bloquer l'accès aux données sensibles
- Transport des données vers l'environnement du serveur d'IBM Tealeaf CX

Déploiement sur site

Le dispositif de capture doit pouvoir accéder à l'intégralité du trafic envoyé au routeur d'équilibrage de charge ou à un segment de réseau contenant le groupe de serveurs d'applications et de serveurs Web pris en charge par la solution d'IBM Tealeaf CX.

Du fait que l'hôte Tealeaf Passive Capture est connecté directement au dispositif de collecte, il n'est pas nécessaire d'ouvrir les ports de pare-feu pour collecter les données.

Les diagrammes suivants illustrent les architectures de déploiement courantes pour les méthodes de collecte par les ports de surveillance des commutateurs ou les TAP réseaux. Les données sont transportées à partir de l'hôte de Passive Capture vers l'environnement de serveur d'IBM Tealeaf CX (via les protocoles TCP/IP ou SSL) où elles sont analysées, rassemblées et archivées.

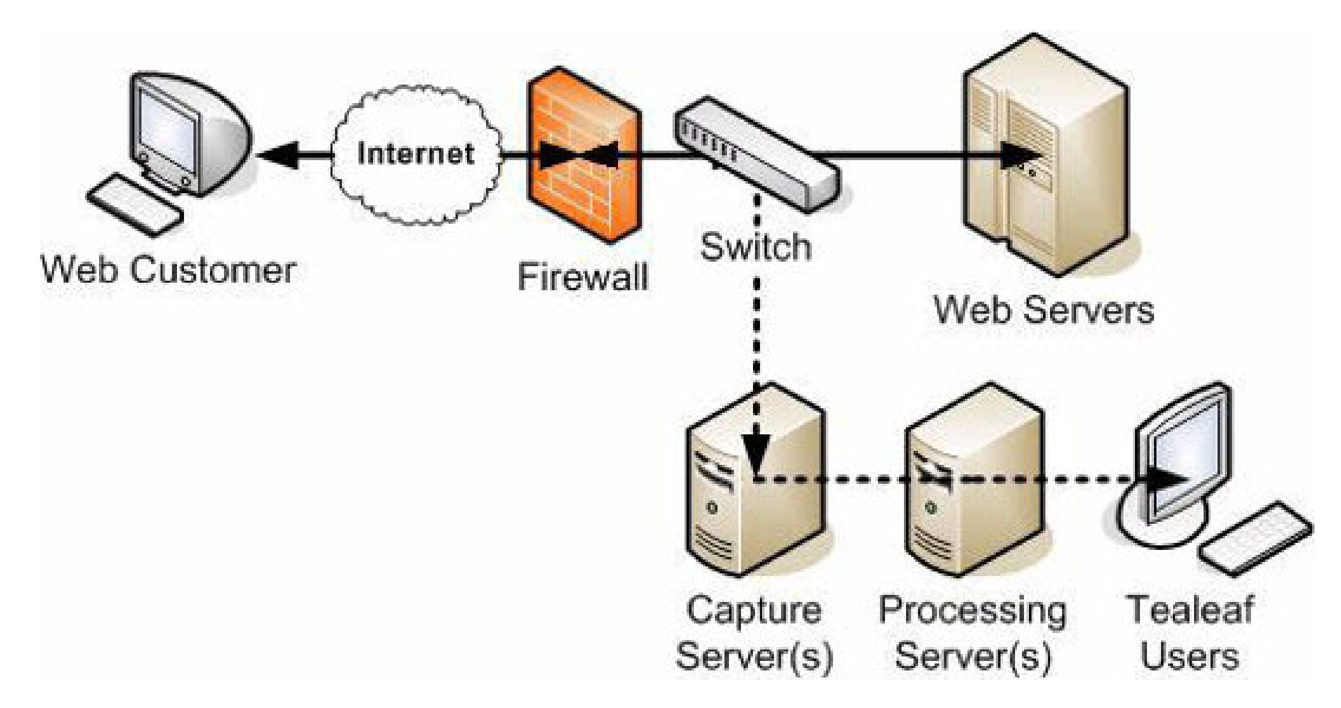


Figure 1. Exemple d'architecture de déploiement - Miroir de port à partir d'un commutateur (ou système d'équilibrage de charge)

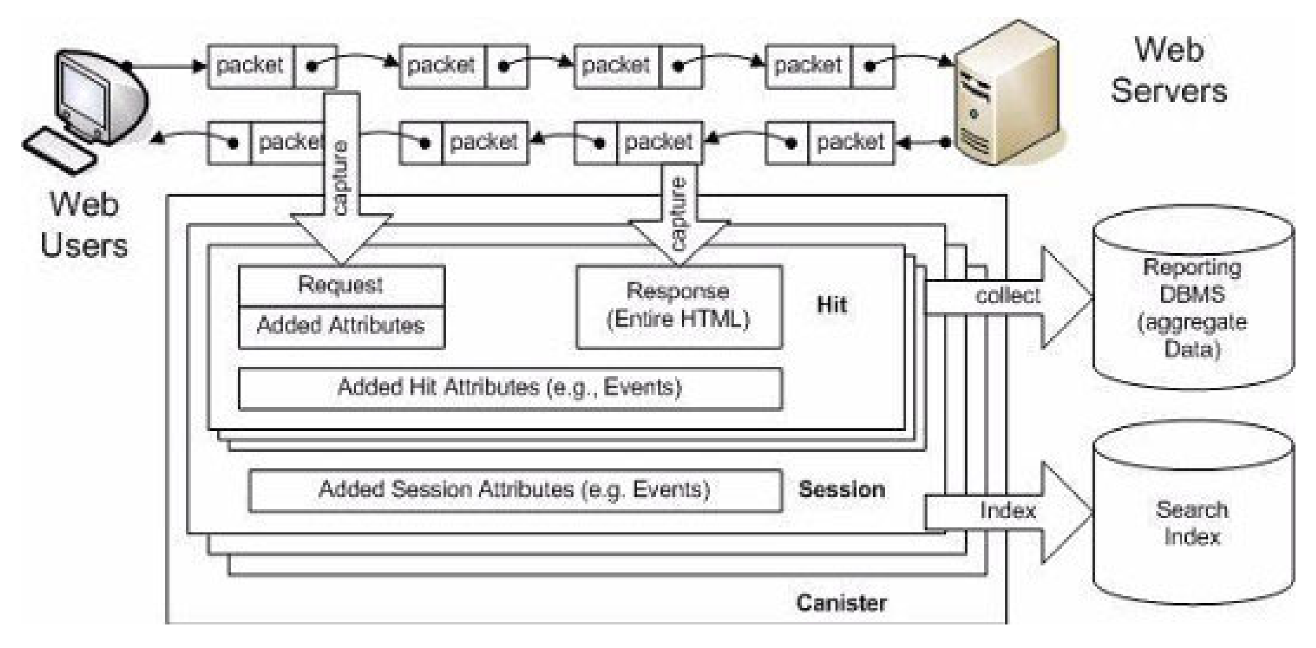
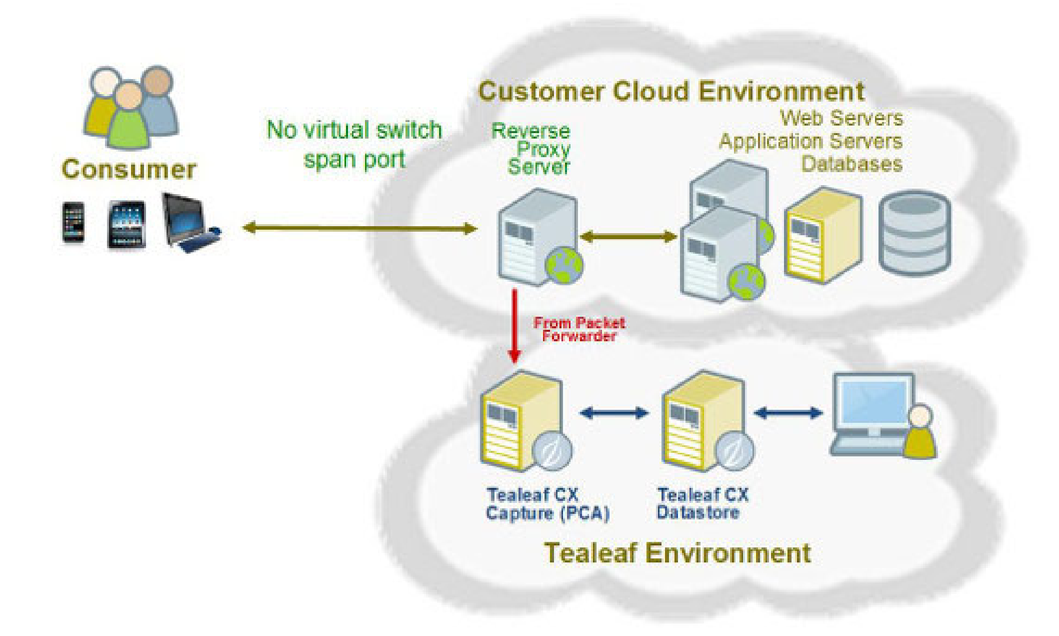


Figure 2. Exemple d'architecture de déploiement - TAP réseau

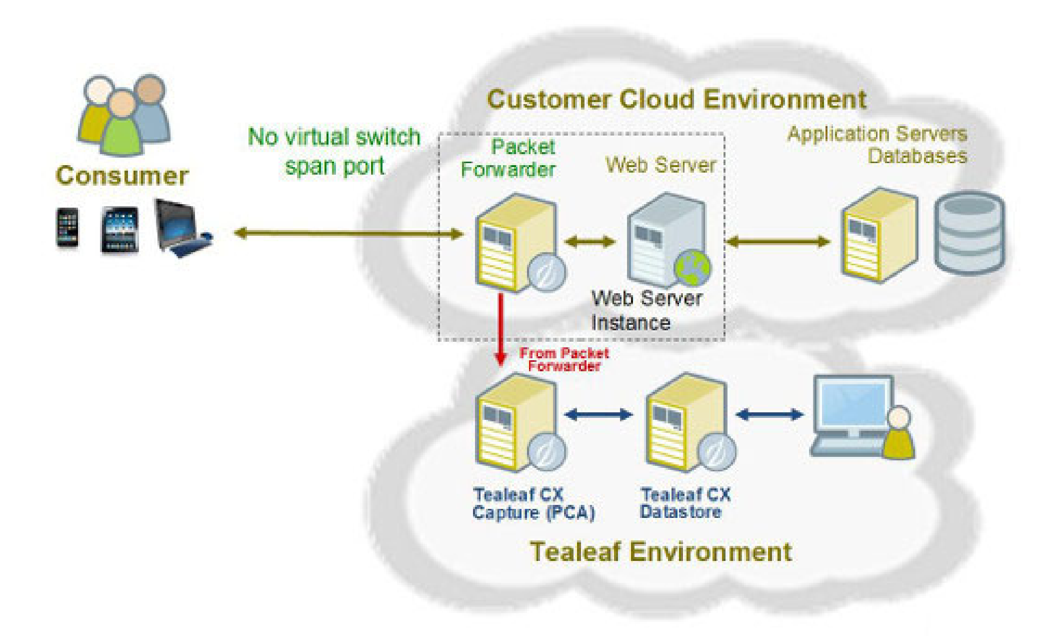
Déploiement dans le Cloud Amazon Web Services (AWS)

Le diagramme suivant illustre l'architecture de déploiement pour Amazon Web Services (AWS) cloud basé sur les installations à l'aide d'un serveur proxy inverse qui dispose également d'un IBM Tealeaf Packet Forwarder installé sur celui-ci. Dans ce déploiement, le IBM Tealeaf Packet Forwarder capture le trafic Web du réseau virtuel au serveur proxy inverse et envoie les données capturées dans le Application de capture passive CX qui est hébergé sur une machine virtuelle séparée.



Le diagramme suivant illustre l'architecture de déploiement pour les installations basées sur le Cloud Amazon Web Services (AWS) où le IBM Tealeaf Packet

Forwarder est déployé sur le serveur Web. Dans ce scénario, chaque instance de serveur Web comporte une instance Packet Forwarder déployée sur le serveur Web. Chaque instance Packet Forwarder capture le trafic Web entre le serveur Web et le client. Packet Forwarder envoie le trafic Web capturé sur le Application de capture passive CX hébergé sur une machine virtuelle séparée.



Pour plus d'informations sur l'installation du IBM Tealeaf Packet Forwarder, voir «Présentation de Packet Forwarder», à la page 6 et «Installation du produit Packet Forwarder», à la page 26.

Capacité de traitement de la PCA

La capacité de traitement des données de hits transférées d'IBM Tealeaf Application de capture passive CX dépend de plusieurs facteurs, dont les suivants :

1. Cartes d'interface réseau : la carte réseau représente la capacité maximale qu'une instance spécifique du serveur PCA peut capturer et traiter. Par exemple, l'utilisation d'une carte réseau d'un débit de 100 mégabits/seconde limite la capacité de traitement maximale pour un serveur PCA en comparaison à des cartes réseau d'1 gigabit/seconde qui permettent le traitement d'un volume de données dix fois plus important.

   Remarque : Tealeaf recommande des cartes d'interface réseau d'au moins 1 gigabit.
2. Coeurs de processeurs : pour être la plus avantageuse possible, la PCA doit être installée sur un serveur avec au moins huit processeurs. Avec plus de coeurs disponibles, vous pouvez installer plus d'instances d'IBM Tealeaf Application de capture passive CX.

   Remarque : Tealeaf recommande l'installation de la PCA sur un système disposant d'au moins huit coeurs.

3. RAM : de la mémoire vive (RAM) supplémentaire sur le serveur PCA offre plus de ressources pour le traitement et la capture des données.
4. SSL : le trafic sécurisé utilise beaucoup de ressources de processeur et peut avoir un impact considérable sur la capacité générale de traitement. Par exemple, une PCA peut gérer une capacité de traitement de 700 mégabits/seconde pour un trafic non SSL alors que cette capacité peut descendre jusqu'à 70 mégabits/seconde pour le même trafic protégé par le protocole SSL.

Tous les paramètres ci-dessus peuvent considérablement limiter la capacité de traitement du logiciel IBM Tealeaf Application de capture passive CX dans son intégralité. Par exemple, si la PCA peut gérer une capacité de traitement effective de 700 mégabits/seconde alors que la bande passante de sa carte d'interface réseau matérielle a 100 mégabits de bande passante, c'est alors la carte d'interface réseau qui fixe la limite et non la PCA.

Présentation de Packet Forwarder

Packet Forwarder sert à capturer et transférer des hits vers un CX PCA basé sur le Cloud qui fonctionne sur une machine virtuelle.

CX PCA traite les hits transférés par Packet Forwarder.

Le logiciel Packet Forwarder est inclus avec CX PCA et se compose d'un composant émetteur et d'un composant destinataire. L'émetteur capture les paquets TCP et les transmet au récepteur désigné. Le récepteur peut être configuré pour capturer des données qui soumises à partir d'un émetteur spécifié. Vous pouvez configurer plusieurs instances de l'émetteur pour envoyer des données à un centralisé CX PCA. Chaque instance de l'émetteur doit se connecter à une instance de récepteur individuel sur le CX PCA.

Remarque : Les instances de l'émetteur et un récepteur instances ne peuvent pas partager le même port d'écoute.

Le serveur Packet Forwarder fournit la fonctionnalité suivante :
- Remplace le composant renifleur de paquets TCP par défaut de la PCA avec un module d'écoute de socket réseau
- Dirige le trafic vers une instance de PCA interne. L'émetteur pointe vers une instance de PCA centralisée dans le Cloud et envoie des paquets vers le récepteur via une connexion réseau.
- Les paquets TCP sont capturés par la détection pour l'écoute du port indiqué.

Les composants Packet Forwarder peuvent être déployés dans un Cloud public ou privé pour gérer la capture et l'émission de paquets TCP pour le traitement par une installation basée sur le Cloud IBM Tealeaf .

Architecture du logiciel

Le logiciel Passive Capture est constitué de trois composants :
1. Les processus de capture des coeurs
2. Un programme de maintenance utilisant le service cron
3. Une console Web en option.

Processus de capture

Le processus de capture des coeurs permet de capturer, rassembler, post-traiter et distribuer les hits HTTP/HTTPS rassemblés au service de transport Tealeaf en cours d'exécution sur un autre poste de travail. Les cinq processus se nomment, dans l'ordre de traitement pendant la capture, captured, listend, reassd, pipelined et deliverd.

- Le processus tcld peut éventuellement se trouver dans votre version de la PCA.

Captured

Captured est le processus de capture de niveau supérieur. Il est le processus parent des processus enfant suivants : listend, reassd, pipelined, and deliverd. Ses deux rôles principaux sont de créer des instances de capture et de créer et gérer ses processus enfant. Une instance de capture est constituée de la paire de processus listend et reassd qui capture et réassemble le trafic réseau. Dès le démarrage, captured crée toutes les instances de capture configurées en tant que processus enfant. Il crée ensuite les processus enfant pipelined et deliverd. Captured redémarre les processus enfant lorsqu'ils s'arrêtent inopinément ou que son script de maintenance décide qu'un processus n'est pas en bon état.

Listend

La fonction première de `Listend` est de capturer les paquets de trafic réseau des interfaces configurées principales et secondaires et de les envoyer au processus de réassemblage, `Reassd`. `Listend` est principalement un renifleur de paquets. Il utilise le trafic configuré et le trafic ignoré afin de déterminer les paquets à capturer. `Listend` met en mémoire tampon les paquets qu'il envoie à `Reassd` afin de gérer les légers retards que prend `Reassd` pour lire les paquets. De plus, `Listend` fournit un paquet d'archivage qui permet d'enregistrer les paquets capturés dans des fichiers sur le disque dur local.

Reassd

La fonction première de reassd est de réassembler les paquets TCP, de déchiffrer le trafic SSL et de faire une analyse initiale des demandes et des réponses HTTP qui en découlent. Reassd extrait des paquets de son canal de communication à l'aide du processus listend pour réassemblage. Après avoir analysé une paire de demande et réponse HTTP, reassd envoie le hit réassemblé à pipelined. Reassd est le processus majeur de Passive Capture et généralement celui qui utilise le plus de ressources de processeur en raison de son traitement des protocoles HTTP et SSL.

Pipelined

La fonction première de pipelined est de récupérer les demandes et réponses HTTP une fois réassemblées par reassd, de les formater en hit Tealeaf et d'effectuer tous les post-traitements de configuration. Durant le post-traitement, il peut abandonner des hits basés sur des options configurables, effectuer de la compression/ décompression de données, bloquer et filtrer l'accès aux données ainsi qu'ordonner à deliverd d'envoyer le hit à un poste de travail. Le poste de travail exécute le service de transport Tealeaf, qui est généralement le serveur IBM Tealeaf CX.

- PCA prend en charge la création de plusieurs instances du processus pipelined. Voir «Processus de pipeline à plusieurs instances», à la page 9.

Routerd

La principale fonction de `Routerd` est l'équilibrage de charge transparent (TLB) des paquets réseau entrants et des connexions aux instances de processus `Reassd`

multiples. Le fait de distribuer le trafic réseau plus uniformément sur toutes les instances `Reassd` augmente l'efficacité des coeurs de processeur du système, ce qui améliore les performances globales. Ce module de processus n'est présent que si le mode TLB est activé. Pour plus d'informations, voir «Présentation de l'équilibrage de charge transparent de d'CX PCA».

Tcld

La fonction première de tcld est de fournir un traitement de script basé sur le langage TCL afin de gérer les hits Tealeaf pour une distribution spécialisée avec le processus deliverd. Ce processus peut accepter les hits Tealeaf provenant d'un ou de plusieurs processus pipelined source.

Deliverd

La fonction première de deliverd est de distribuer les hits Tealeaf une fois formatés vers au minimum un service de transport Tealeaf sur des postes de travail à distance comme tcld lui en a donné l'ordre. C'est tcld qui décide si un hit doit être envoyé et où il doit être envoyé. Deliverd, lui, établit la connexion réseau et envoie les hits sur le réseau au service de transport Tealeaf. Il peut éventuellement communiquer avec le service de transport Tealeaf à l'aide d'une connexion SSL afin d'offrir un canal sécurisé.

Failoverd

Ce processus facultatif est présent lorsque la fonction de basculement est activée et qu'elle s'exécute sur une instance d'IBM Tealeaf Application de capture passive CX.

- Il envoie des signaux de présence aux processus failoverd sur d'autres instances PCA de l'environnement.
- Il s'exécute indépendamment des autres processus PCA.
- Voir «Console Web de la PCA - Onglet Reprise», à la page 161.

Memcached

Le processus `Memcached` fournit un système de mise en cache global en mémoire à la CX PCA. `Memcached` permet essentiellement de stocker des informations de session SSL pour que toutes les instances `Reassd` y accèdent ultérieurement pour traiter le déchiffrement SSL (sessions SSL reprises). Ce module de processus n'est présent que si le mode TLB est activé.

Pour plus d'informations, voir «Présentation de l'équilibrage de charge transparent de d'CX PCA».

Présentation de l'équilibrage de charge transparent de d'CX PCA

La CX PCA peut être configurée pour l'équilibrage de charge transparent (TLB) qui permet la segmentation et la distribution transparentes du trafic réseau de capture. L'équilibrage de charge transparent est activé par défaut dans les nouvelles installations de la CX PCA. Avant cette fonctionnalité (mode sans équilibrage de charge transparent), la segmentation du trafic de capture nécessitait l'affectation de blocs de trafic à des instances spécifiques de la CX PCA pour le traitement doté de l'équilibrage de charge.

En configurant la CX PCA pour l'équilibrage de charge transparent, vous pouvez :

- Réduire les problèmes de support clientèle qui sont occasionnés par des charges de trafic non uniformes ou des modifications apportées au profil de trafic sur plusieurs instances de la CX PCA dans lesquelles une augmentation soudaine du

trafic réseau peut surcharger une instance de la CX PCA. Si une instance de la CX PCA est surchargée, l'instance peut redémarrer et perdre le trafic capturé. En activant l'équilibrage de charge transparent, le trafic réseau est distribué aux instances de la CX PCA en mode circulaire. La distribution du trafic réseau aux instances de la CX PCA empêche la surcharge d'une instance.

- Simplifier l'installation et la configuration de la CX PCA. En activant l'équilibrage de charge transparent, vous n'avez pas besoin de fournir une configuration supplémentaire pour chaque instance de CX PCA supplémentaire. Vous pouvez définir le nombre d'instances à utiliser et Tealeaf distribue automatiquement le trafic réseau aux instances.
- Capturer le trafic à partir d'une adresse IP virtuelle (VIP) unique pour les serveurs Web configurés pour fonctionner sous une VIP unique.

Instances multiples

En mode sans équilibrage de charge transparent, la CX PCA peut être configurée pour lancer plusieurs instances des processus `listend` et `reassd` afin qu'ils utilisent plusieurs coeurs de processeur afin de gérer d'importantes charges de trafic de capture. Les instances peuvent être configurées afin de capturer des adresses et ports TCP/IP différents pour distribuer la charge de trafic aux instances de capture. Les instances peuvent partager des cartes d'interface réseau pour la capture des paquets ou capturer des paquets en utilisant plus de cartes réseau disponibles sur le serveur d'IBM Tealeaf Application de capture passive CX.

La CX PCA peut aussi créer plusieurs instances de processus pipelined afin de répartir la charge à traiter.

En mode TLB, une instance unique de `listend` est utilisée pour alimenter plusieurs processus `reassd` via le processus `routerd`. Plusieurs instances sont fournies via les processus `reassd` lorsque le travail est requis et élimine la charge de travail manuelle de segmentation et de distribution de la charge de trafic de capture.

Pour l'intégration aux serveurs Web dotés de l'équilibrage de charge qui utilisent une adresse IP virtuelle (VIP) unique, voir «Présentation de l'équilibrage de charge transparent de d'CX PCA», à la page 8.

Processus de pipeline à plusieurs instances

Remarque : Les build 3403 et ultérieures de la PCA prennent en charge plusieurs instances du processus pipelined.

Le processus pipelined exécute plusieurs opérations gourmandes en ressources du processeur, comme par exemple les activités de blocage de données confidentielles, celles-ci pouvant être à l'origine de goulots d'étranglement dans les configurations à une seule unité d'exécution. Si besoin est, vous pouvez créer plusieurs instances du processus pipelined pour répartir la charge de traitement pour toutes les instances de la PCA sur toutes les ressources disponibles du processeur.

Imaginez par exemple qu'une seule instance de la PCA génère 500 aperçus de page/seconde et qu'elle est configurée pour un traitement intensif de la confidentialité du pipeline, ce qui limite sa capacité de traitement à 200 aperçus de page/seconde. L'ajout de deux instances de pipeline supplémentaires (pour un total de trois pipelines) permet de traiter le débit global d'aperçus de page.

Au moins un processus reassd (plusieurs instances de la PCA) peut alimenter, avec les hits HTTP qui en résultent, une seule file d'attente de mémoire partagée (SHM) qui gère la répartition vers les instances disponibles des processus pipelined en mode circulaire.

Imaginez, pour un cas de plusieurs instances de la PCA, que vous en avez créé quatre et que celles-ci génèrent au total 1000 aperçus de page/seconde. Si dans votre environnement, un pipeline peut traiter à lui seul 400 aperçus de page/seconde, vous pouvez alors ajouter deux autres pipelines pour traiter le volume entier.

Le basculement maître-esclave de la PCA prend aussi en charge plusieurs instances de pipelines. Voir «Console Web de la PCA - Onglet Reprise», à la page 161.

Pour plus d'informations sur la configuration de plusieurs instances du processus pipelined, voir «Console Web de la PCA - Onglet Pipeline», à la page 101.

Cartes d'un pipeline à plusieurs instances

Lorsque plusieurs instances du pipeline sont déployées, les processus pipelined supplémentaires sont intégrés dans le pipeline principal de la manière suivante :

```
        pipe         queue            queue2      pipe
listend ---> reassd >+->-+> pipelined >-+--> tcld <--> deliverd
  ...               |   |     ...     |
listend ---> reassd >+   +> pipelined >-+
```

Programme de maintenance

Le logiciel Passive Capture comprend un programme de maintenance à exécuter en tant qu'utilisateur racine via le service cron sur le poste de travail. Le programme de maintenance effectue plusieurs tâches, y compris la vérification du bon fonctionnement des processus de capture, la consignation, l'établissement des statistiques, l'envoi des statistiques de diagnostic à un autre poste de travail et la gestion de plusieurs fichiers journaux créés par les programmes de Passive Capture.

Console Web

La console Web est disponible via un serveur Web interne compris dans le logiciel Passive Capture. Elle fournit une interface basée sur navigateur pour la configuration et la gestion de Passive Capture. Le serveur Web fournit aussi une adresse URL utilisable par l'utilitaire du statut du portail. L'utilitaire du statut du portail récupère les contenus de l'URL pour contrôler l'intégrité et l'état du serveur d'IBM Tealeaf Application de capture passive CX.

- La console Web et son serveur Web sont facultatifs et peuvent être désactivés. Voir «Navigateurs pris en charge pour la console Web de la PCA», à la page 54.

Logiciel tiers

Les packs d'installation de Passive Capture comprennent les packs tiers suivants :

```
Apache HTTPD 2.2.19
Expat 1.2
LibNet 1.1.1
LibPCAP 1.1.1
OpenSSL 1.0.0d
```

```
PHP 5.2.9
TCL 8.4.x
Tcpdump 4.1.1
Tcpslice 2004.05.10
```

Certains d'entre eux sont utilisés par le logiciel Tealeaf directement et d'autres sont fournis comme outils de gestion du système.

Commandes de ce manuel

Les commandes Linux de ce manuel peuvent être formatées à des fins d'affichage. Voici les méthodes reconnues pour le faire.

Par exemple, la commande suivante apparaît sur l'écran :

```
# tcpdump -Xnr tst1.dmp |more
```

Pour un meilleur affichage, vous pouvez saisir la commande manuellement de la manière suivante :

```
# tcpdump -Xnr \
tst1.dmp |more
```

Remarquez la barre oblique inversée, celle-ci indique que la ligne continue.

Les commandes qui s'affichent sur l'écran peuvent être formatées de la manière suivante :

```
# tcpdump -Xnr \
> tst1.dmp |more
```

Remarquez le caret (>) au début de la deuxième ligne pour indiquer que la ligne de commande continue.

Remarque : Veillez à copier et coller les commandes Linux correctement à partir du manuel. Certaines peuvent nécessiter une modification.

Besoins du trafic de capture du réseau Tealeaf PCA

Cette section présente les conditions nécessaires à Tealeaf pour traiter le trafic réseau miroir et le transférer à la PCA pour la capture.

Les périphériques réseau comme les miroirs de ports de commutateurs, les TAP réseaux et les dispositifs d'équilibrage de charge ne sont que quelques-uns des points de capture du trafic réseau qui peuvent fournir une copie du trafic réseau en temps réel à IBM Tealeaf Application de capture passive CX. En général, le trafic miroir correspond au trafic du serveur Web du site Internet du client.

- Le trafic réseau miroir est considéré comme passif par nature puisque les cartes d'interface réseau de la PCA consacrées à la capture n'interagissent pas avec le trafic réseau opérationnel.

Remarque : IBM Tealeaf Application de capture passive CX prend en charge la capture d'un trafic SSL 128 bits. Les méthodes de chiffrement qui utilisent le moins de chiffres possible pour les bits de chiffrement ne sont pas prises en charge.

Conditions de base nécessaires au trafic

Pour que la PCA s'exécute correctement, elle a besoin d'un trafic réseau miroir qui soit de haute intégrité et de haute qualité. Toute perte de paquets réseau TCP critiques peut empêcher la PCA de réassembler le trafic TCP en hits HTTP. Les paquets TCP perdus peuvent entraîner, dans les sessions Tealeaf, des pages manquantes ou incomplètes, parfois même les deux. Dans le pire des cas, la session toute entière peut être inutilisable.

Vérifiez que les conditions de base sont respectées avec votre administrateur de réseau :

1. Flux de trafic : la PCA a besoin d'un flux de trafic bidirectionnel ou de deux flux unidirectionnels contenant tout le trafic de demandes et de réponses HTTP entre votre application Web et les navigateurs visiteurs avec lesquels elle interagit.
2. Aucune erreur sur des paquets, aucun paquet abandonné : pas d'erreurs, de paquets abandonnés ou surchargés sur la carte d'interface réseau du système d'exploitation et au niveau du réseau
   - Une commande `ifconfig ethX` sur la carte d'interface réseau de la capture doit afficher un nombre constant de paquets abandonnés ou d'erreurs.
   - Si le nombre augmente considérablement, il se peut qu'il y ait des problèmes avec la fidélité du trafic envoyé à la PCA. La taille de votre matériel PCA peut aussi ne pas correspondre à votre volume de trafic, il se peut même que les deux cas de figure se présentent.
3. Adresse IP réelle du visiteur : le point de capture peut voir l'adresse IP réelle du visiteur ou l'adresse hôte réelle de l'IP du visiteur.
   - L'accès à l'adresse IP réelle de vos visiteurs peut s'avérer être une ressource précieuse pour le traitement des incidents. Pour les clients qui utilisent des dispositifs d'équilibrage de charge, cette condition n'est pas applicable.
4. Trafic filtré : le trafic miroir est filtré pour ne garder que le trafic essentiel.
   - Tealeaf recommande de rejeter le maximum de trafic inutile au niveau du réseau avant de le distribuer à la PCA. Ce filtrage décharge les ressources de traitement que la PCA doit utiliser pour rejeter le trafic.
5. Anomalies relatives aux connexions TCP permanentes :
   - Pour capturer le trafic, la PCA doit voir le démarrage de toutes les connexions TCP. Voir «Connexions TCP», à la page 13.

Chiffrement Diffie-Hellman

Diffie-Hellman est un type de chiffrement SSL. Il a été conçu pour que les logiciels tiers, qui sont différent des systèmes autres que les systèmes situés aux deux extrémités d'une conversation, ne puissent pas déchiffrer le trafic des communications. IBM Tealeaf Application de capture passive CX ne peut pas capturer une session utilisateur établie avec un serveur Web à l'aide de ce chiffrement.

Remarque : Tealeaf ne prend pas en charge l'utilisation du protocole de chiffrement Diffie-Hellman et vous recommande de configurer vos serveurs Web afin qu'ils ne l'utilisent pas.

Voir «Comment retirer le système de chiffrement Diffie-Hellman de la liste des chiffrements SSL de serveur Web ?», à la page 273.

Extension de tickets de session TLS

Cette extension du protocole SSL est utilisée par certains serveurs Web pour transmettre un trafic chiffré aux navigateurs qui le prennent en charge. Dans les modules OpenSSL des serveurs Web Apache les plus récents et probablement d'autres serveurs Web, la nouvelle extension du protocole SSL TLS (RFC-5077) connue sous le nom d'extension de tickets de session, qui permet la reprise d'une session sans état, chiffre les informations sur l'état du SSL uniquement utilisées lorsque le navigateur client et le serveur Web respectent tous les deux les normes.

Remarque : Les versions récentes d'IBM Tealeaf Application de capture passive CX prennent en charge l'extension de tickets de session SSL. Si vous activez cette extension sur votre serveur Web, vérifiez que vous avez installé la build `TLSv1.x in Build 3327` ou version ultérieure ou que vous l'avez mise à niveau vers cette build. Pour plus d'informations sur le téléchargement d'IBM Tealeaf , voir IBM® Passport Advantage Online.

Voir «Certains hits SSL n'apparaissent pas dans les sessions de navigation de Firefox», à la page 275.

Connexions TCP

Vérifiez avec votre équipe informatique si la connexion TCP permanente est activée dans votre infrastructure informatique. Les connexions TCP permanentes individuelles peuvent être utilisées par plusieurs visiteurs de votre application Web. Elles peuvent aussi être déployées par un système d'équilibrage de charge tel qu'un périphérique réseau F5, par un proxy frontal tel qu'un serveur Akamai ou par le serveur Web lui-même.

IBM Tealeaf Application de capture passive CX a besoin de contrôler le démarrage de chaque connexion TCP. Si les connexions TCP permanentes sont activées, la PCA peut alors réassembler des hits depuis des connexions en cours.

Pour les sessions SSL, le regroupement des transactions SSL en pool est un bon moyen d'optimiser le processus. Cependant, le regroupement des transactions SSL en pool sur un ensemble de connexions TCP permanentes peut engendrer des anomalies qui empêchent ces sessions d'être déchiffrées. Si une nouvelle session SSL n'apparaît pas pour permettre à la PCA de mettre les informations sur l'ID des sessions SSL en mémoire cache, alors aucune des sessions SSL qui réutilisent l'ID de session ne peuvent être déchiffrées.

Dans un tel environnement, les connexions peuvent durer jusqu'à 24 heures, ce qui engendre un délai dans la capture de sessions quand la PCA est installée, mise à niveau ou redémarrée. Certains paramètres de configuration de solutions ou de compromis sur les dispositifs de réseau source permettent éventuellement d'atténuer/réduire le délai d'attente.

- Pour plus informations, contactez votre équipe informatique.

Données dupliquées

Chaque instance d'IBM Tealeaf Application de capture passive CX doit fournir des données uniques à Tealeaf.

Remarque : Les données dupliquées ne doivent pas être transférées volontairement à Tealeaf. Alors que la PCA a été conçue pour rejeter les données dupliquées, les paquets dupliqués inutiles peuvent ralentir, dans un environnement volumineux, le processus de traitement. Tealeaf prend en charge le basculement passif vers

plusieurs instances d'IBM Tealeaf Application de capture passive CX. Voir «Console Web de la PCA - Onglet Reprise», à la page 161.

Origine des anomalies relatives à la qualité du trafic réseau

Dans cette section, vous en apprendrez plus sur les anomalies relatives à la qualité du trafic réseau.

Paquets réseau TCP abandonnés

Les paquets réseau TCP peuvent être abandonnés si l'un des cas de figure exposé ci-dessous se présente. D'autres situations, plus rares, peuvent se présenter.

Miroir de port saturé

Les paquets réseau peuvent être abandonnés en raison d'un miroir de port de commutateur réseau saturé. Ce cas se produit lorsqu'au moins l'un des flux de trafic réseau sélectionnés est configuré pour partager un seul port alors que la somme de tout le trafic sélectionné dépasse la bande passante de ce port. Par exemple, trois flux de trafic miroir de 500 mégabits/seconde avec une bande passante globale de 1,5 gigabits/seconde sont envoyés à un miroir de port de commutateur qui ne peut traiter qu'un trafic de 1 gigabit/seconde. Pendant les pics de trafic, ce miroir de port est incapable de traiter la charge et les paquets sont abandonnés.

Ressources de processeur inappropriées sur le commutateur

Le miroir de port peut dépendre du processeur du commutateur en ce qui concerne les cycles disponibles pour le regroupement et/ou filtrage du trafic nécessaire à la mise en miroir.

Les commutateurs actuels attribuent généralement des cycles processeur disponibles pour la mise en miroir du port tandis que la priorité du processeur est de traiter les opérations du commutateur. Si le processeur est occupé avec les opérations du commutateur, il n'y aura pas assez de cycles pour gérer la mise en miroir et, dans ce cas, les opérations de mise en miroir de port seront "affamées" et les paquets réseau seront abandonnés dans le trafic miroir.

Remarque : La bande passante du trafic miroir ne doit pas s'approcher des limites réelles du miroir de port. Une courbe d'utilisation d'un commutateur réseau devient alors un facteur déterminant pour la mise à disposition d'un trafic réseau de haute intégrité.

Autres périphériques réseau

Dans une infrastructure réseau plus complexe, il peut exister davantage de périphériques réseau avec une source de trafic réseau miroir, comme par exemple des dispositifs servant au rassemblement du trafic réseau ou à la réplication de ports. Ces types de périphériques peuvent entraîner une perte de paquets réseau, tout particulièrement si l'un des périphériques actifs altère le trafic réseau pendant sa phase de traitement.

Trafic unidirectionnel

Une simple erreur dans la configuration et la PCA peut recevoir un trafic réseau unidirectionnel uniquement. Dans ces cas-là, ce sont soit les demandes HTTP, soit les réponses HTTP qui sont transmises à la PCA, mais pas les deux.

Pour que la PCA puisse correctement réassembler les hits HTTP, le trafic TCP doit être fourni dans les deux directions. La plupart du temps, cette situation est assez facile à identifier et est généralement due à une erreur dans la configuration du périphérique réseau source.

Evaluation du nombre de paquets abandonnés

Malheureusement, peu de valeurs relatives au commutateur réseau permettent d'indiquer si les mémoires tampons d'un commutateur sont surchargées, ce qui peut entraîner un abandon de paquets réseau.

Des éléments comme la bande passante du port et l'utilisation du processeur permettent d'indiquer indirectement une anomalie éventuelle. Ces indicateurs testent l'état du commutateur réseau à des intervalles de temps prédéfinis. Cependant, si un pic arrive entre deux périodes de test, aucune information ne sera disponible.

La PCA fournit plusieurs indicateurs pouvant identifier les conditions d'abdandon des paquets réseau. Ces indicateurs sont les seuls éléments de données qui permettent d'évaluer les causes probables de l'abandon de paquets.

Le meilleur indicateur reste l'évaluation des sessions de Tealeaf capturées, à la recherche de pages manquantes et/ou incomplètes. La validation statique des sessions de test de Tealeaf peut fournir un autre élément de données en analysant la raison pour laquelle il existe des pages manquantes dans les sessions. Le suivi en temps réel des sessions de Tealeaf avec des événements composés qui déclenchent l'apparition de pages manquantes peut permettre de déterminer s'il existe une solution pour remédier au problème.

- D'autres outils de diagnostic et d'autres méthodes peuvent permettre de résoudre le problème. Voir "Traitement des incidents - Capture" dans le manuel de dépannage d'*IBM Tealeaf*.

Chapitre 2. Installation

Remarque : Actuellement, les builds 3500 et ultérieures de la PCA ne doivent être déployées que si votre environnement répond aux conditions suivantes :

- Les adresses IPv6 doivent être capturées. Le traitement des adresses IPv6 via la solution Tealeaf est uniquement disponible pour les versions 8.4 et ultérieures.
- Vos serveurs Apache gèrent la compression du trafic SSL vers et à partir des navigateurs Chrome.
- Pour la prise en charge de HTTP_X_FORWARDING, vous devez utiliser la version 3502 ou une version plus récente de la PCA.
- Pour plus d'informations sur les versions 35xx de la PCA, contactez Tealeaf http://support.tealeaf.com.

Ce chapitre décrit l'installation du logiciel Tealeaf Passive Capture sur Red Hat Enterprise Linux (RHEL).

Remarque : Si vous effectuez une mise à niveau à partir d'une version antérieure de la PCA, reportez-vous d'abord au bas de la page «Remarques relatives à la mise à niveau de la PCA», à la page 34.

Liste de vérification de préinstallation

Vous devez suivre les instructions suivantes avant d'installer IBM Tealeaf Application de capture passive CX et Packet Forwarder.

Configuration du trafic réseau

Avant de commencer, vous devez consulter les exigences concernant le trafic réseau dont la PCA a besoin. Cette information doit être partagée avec l'équipe d'infrastructure informatique.

Remarque : Tealeaf ne prend pas en charge l'utilisation du protocole de chiffrement Diffie-Hellman et vous recommande de configurer vos serveurs Web afin qu'ils ne l'utilisent pas.

Remarque : IBM Tealeaf Application de capture passive CX est compatible avec l'extension de tickets de session SSL. Si vous activez cette extension sur votre serveur Web, mettez-la à niveau vers l'une des builds compatibles :

- TLSv1.1 build 3611 ou ultérieure
- TLSv1.2 build 3611 ou ultérieure

Pour plus d'informations sur le téléchargement d'IBM Tealeaf , voir IBM Passport Advantage Online.

Remarque : IBM Tealeaf Application de capture passive CX attend de voir toutes les connexions TCP démarrer. Si l'un des serveurs fournissant des données à la PCA utilise les connexions TCP permanentes, cela peut entraîner un délai d'attente dans le processus de capture de sessions ainsi qu'une perte de données. Voir «Besoins du trafic de capture du réseau Tealeaf PCA», à la page 11.

Voir «Besoins du trafic de capture du réseau Tealeaf PCA», à la page 11.

Configuration matérielle

Voici la configuration matérielle requise pour IBM Tealeaf Application de capture passive CX.

Configuration recommandée

Remarque : Les recommandations suivantes s'appliquent à la build 3403 de la PCA ainsi qu'aux versions plus récentes.

Pour l'installation d'IBM Tealeaf Application de capture passive CX, Tealeaf recommande le matériel suivant :

- Bi-processeur, quadricoeur : processeur Intel quad-core Xeon à 2,8 GHz minimum pour un total de huit coeurs minimum
- 16 Go de RAM minimum
- 3 cartes réseau de 1 gigaoctet chacune
- Un disque dur SAS ou SCSI de 100 Go minimum
  - Une durée d'accès de 15 ms
  - Une vitesse de 7200 tr/mn

Voici le matériel recommandé pour l'installation de logiciels et pour la récupération de la machine :

- Un lecteur de CD-ROM
- Un lecteur de disquette de 1,44 Mo
- Un deuxième lecteur pour la capture et le stockage du trafic réseau dans les archives : entre 200 Go et 800 Go

Exigences minimales

Le logiciel Tealeaf Passive Capture nécessite au minimum le matériel suivant :

Remarque : Voici les exigences minimales pour l'exécution du logiciel Passive Capture. Celles-ci ne permettront pas la prise en charge du volume de données et des besoins en traitement de votre environnement. Pour plus d'informations sur le dimensionnement de votre environnement, contactez les services professionnels de Tealeaf.

- Bi-processeur, quadricoeur : processeur Intel dual-core Xeon à 2,8 GHz minimum pour un total d'au moins quatre coeurs
- 8 Go de RAM minimum
- 3 cartes réseau d'1 gigaoctet chacune
- Un disque dur SAS ou SCSI de 100 Go minimum
  - Une durée d'accès de 15 ms
  - Une vitesse de 7200 tr/mn

Cartes accélératrices prises en charge

Voir Annexe B, «Annexe - Cartes accélératrices prises en charge», à la page 249.

Intégration avec des modules de sécurité matérielle

Il est possible d'intégrer Tealeaf PCA avec des clés privées contenues dans les modules de sécurité matérielle. VoirAnnexe D, «Annexe - Intégration des clés SSL de Tealeaf avec HSM», à la page 253.

Configuration du système d'exploitation

Avant de procéder à l'installation d'IBM Tealeaf Application de capture passive CX, vous devez installer Red Hat Enterprise Linux ou SUSE Linux Enterprise Server. Pour plus d'informations, voir Chapitre 9, «Configuration matérielle et installation du système d'exploitation», à la page 235.

Distributions de système d'exploitation prises en charge pour des builds CX PCA

Remarque : Si votre serveur CX PCA exécute une build antérieure à la build 3502, il est recommandé de procéder à la mise à niveau vers la build 3502 ou une build ultérieure. Avant la mise à niveau vers CX PCA build 3502 ou une build ultérieure, vous devez mettre à niveau le système d'exploitation sur votre serveur CX PCA vers une distribution de Linux prise en charge par CX PCA.

Les distributions ci-après de Red Hat Enterprise Linux et SUSE Linux Enterprise Server sont compatibles avec CX PCA build 3502 et les builds ultérieures.

- Red Hat Enterprise Linux (RHEL) versions 5.6 et 6.1
- SUSE Linux Enterprise Server (SLES) versions 11

Remarque : Selon le type de système d'exploitation, des installations supplémentaires peuvent être nécessaires. Examinez l'ensemble des exigences ci-après.

Distributions de système d'exploitation prises en charge pour Packet Forwarder

Pour installer et exécuter le logicielPacket Forwarder, vous devez au moins posséder le système d'exploitation Red Hat Enterprise Linux (RHEL) 6.4. Cette condition s'applique à toutes les architectures de déploiement prises en charge pour Packet Forwarder.

Remarque : Selon le type de système d'exploitation, des installations supplémentaires peuvent être nécessaires. Examinez l'ensemble des exigences ci-après.

Désactivation de `SELinux`

Avant de commencer, SELinux doit être désactivé via le système d'exploitation, et ce, pour toutes les versions de Red Hat Linux. Voir Chapitre 9, «Configuration matérielle et installation du système d'exploitation», à la page 235.

Désactivation des `iptables`

Sur le serveur Linux qui héberge IBM Tealeaf Application de capture passive CX, désactivez l'utilisation des `iptables`. Pour plus d'informations, voir Chapitre 9, «Configuration matérielle et installation du système d'exploitation», à la page 235.

Hyper-Threading

Remarque : Si CX PCA est hébergé sur un serveur qui prend en charge la fonction Hyper-Threading, ne la désactivez pas. Il est activé sur la plupart des serveurs qui le prennent en charge et doit aussi l'être pour IBM Tealeaf Application de capture passive CX.

Si vous utilisez plusieurs instances de CX PCA, ne considérez pas les processeurs virtuels dotés de la technologie Hyper-Threading comme des coeurs de processeur disponibles. Afin de calculer le nombre maximum d'instances de CX PCA, prenez seulement en compte les coeurs de processeur réels. Voir «Instances multiples de la PCA», à la page 22.

Système d'exploitation multicoeur 32 bits

Pour un système multicoeur avec un système d'exploitation 32 bits, le processus d'installation détecte automatiquement les processeurs supplémentaires et installe un noyau SMP afin de permettre la prise en charge de la technologie multicoeur. La prise en charge de l'extension d'adresse physique (PAE) est comprise dans le noyau SMP et prend en charge jusqu'à 16 Go de RAM sur un système d'exploitation 32 bits.

Système d'exploitation multicoeur 64 bits

Pour un système multicoeur avec un système d'exploitation 64 bits, le processus d'installation ne nécessite aucun autre noyau.

Remarque : Les versions 32 bits des bibliothèques nécessaires doivent être installées à partir du disque d'installation de votre version 64 bits de Linux. Voir «Packs nécessaires».

Packs nécessaires

Le RPM de Tealeaf Passive Capture a besoin des packs suivants, compris dans l'installation minimale de RHEL et de SLES. Faisant partie de l'installation du système d'exploitation 32 bits, ces packs doivent déjà être installés.

- Pour les installations 64 bits, vous devez les installer manuellement. Alors que les versions 64 bits de ces bibliothèques sont installées automatiquement, la PCA a besoin des versions 32 bits et celles-ci doivent être disponibles sur le support d'installation.

Remarque : Une installation minimale de Red Hat Enterprise Linux est nécessaire pour l'installation de Tealeaf. Si, à cause des politiques locales concernant les pare-feux ou les logiciels de surveillance, l'installation a besoin de configurations ou de logiciels supplémentaires, ces composants doivent être installés et configurés. Ceci doit être fait une fois que l'installation minimale de Tealeaf est terminée et que Passive Capture est prêt à s'exécuter.

Serveur Red Hat Enterprise Linux édition 5.6

Packs nécessaires :

- bash-3.1-16.1
- coreutils-5.97-12.1.el5
- expat-1.95.8-8.2.1
- gawk-3.1.5-14.el5
- glibc-2.5-18
- libgcc-4.1.2-14.el5
- libgdbm-1.8.0-26.2.1
- libicudata.so.38
  - Fourni avec le RPM de Tealeaf
- libicuuc.so.38

- Fourni avec le RPM de Tealeaf
- libstdc++-4.1.2-14.el5
- libxml2-2.6.26-2.1.2
- perl-5.8.8-10
- zlib-1.2.3-3

Serveur Red Hat Enterprise Linux édition 6.1

Packs nécessaires :
- bash-4.1.2-3.el6.i686
- coreutils-8.4-9.el6.i686
- gawk-3.1.7-6.el6.i686
- glibc-2.12-1.7.el6.i686
- libgcc-4.4.4-13.el6.i686
- libstdc++-4.4.4-13.el6.i686
- libxml2-2.7.6-1.el6.i686
- libicudata.so.38
  - Fourni avec le RPM de Tealeaf
- libicuuc.so.38
  - Fourni avec le RPM de Tealeaf
- openssl-1.0.0-4.el6.i686
- perl-5.10.1-115.el6.i686
- zlib-1.2.3-25.el6.i686

SUSE Linux Enterprise Server 11

Packs nécessaires :
- bash-3.2-147.3
- coreutils-6.12-32.17
- gawk-3.1.6-1.22
- glibc-2.9-13.2
- libgcc43-4.3.3_20081022-11.18
- libstdc++6-4.7.2
- libxml2-2.7.1-10.8
- zlib-1.2.3-106.34

Installation des packs requis

Les packs obligatoires doivent être installés pour la bonne installation du RPM tealeaf-pca.

Remarque : L'installation doit être exécutée par un utilisateur racine. Voir Chapitre 9, «Configuration matérielle et installation du système d'exploitation», à la page 235.

Pour voir les packs requis pour votre machine personnelle, exécutez la commande suivante :

```
rpm -q --requires -p tealeaf-pca-XXXX-1.YYYY.ZZZZ.rpm | fgrep -v rpmlib | \
sort -u | while read x; do rpm -q --whatprovides ${x}; done | sort -u
```

Où :

- XXXX correspond au numéro de build de la PCA
- YYYY correspond à la distribution Linux
- ZZZZ correspond à l'architecture

Si vous ne parvenez pas à trouver les RPM sur le disque ou l'image ISO d'installation, contactez votre administrateur Linux.

Remarque : La plupart des versions de Linux comprennent un système de référentiel RPM automatisé qui localise et met à jour les RPM manquants. RHEL utilise le système de référentiel YUM. SUSE utilise le système de référentiel YAST. Tealeaf ne fournit pas ces RPM.

Recommandations de partitions pour le disque dur

Voici les partitions et les tailles recommandées pour un lecteur de 100 Go pour le logiciel Passive Capture.

Point de montage
Taille

/
4 Go

/archive
Espace disque restant (42 Go)

/tmp
4 Go

/usr
40 Go

/var
8 Go

swap
2 Go

Si elle est activée, la partition /archive est utilisée pour le stockage des archives de paquet brutes. Par défaut, cette fonction est désactivée et ne doit être utilisée qu'en cas de problèmes survenus lors du traitement des incidents.

La partition /usr contient le logiciel Passive Capture. Le RPM du logiciel Tealeaf Passive Capture installe des fichiers dans /usr/local.

Instances multiples de la PCA

Remarque : La formule suivante et les remarques qui lui sont associées doivent servir d'instructions lors de la configuration de plusieurs instances de la PCA. Utilisez-les pour estimer vos besoins et préparez-vous à devoir faire des ajustements en fonction des modèles de trafic et de l'utilisation du processeur.

Vous pouvez installer plusieurs instances d'IBM Tealeaf Application de capture passive CX. Pour calculer le nombre maximum recommandé d'instances de la PCA à installer dans votre environnement Tealeaf, utilisez la formule suivante :

```
Nombre d'instances PCA = nombres de coeurs physiques – nombre de pipelines PCA - 1.
```

Par exemple, si votre environnement contient 16 noyaux physiques, vous pouvez espérer utiliser jusqu'à 15 instances de la PCA.

Remarque : Pour chaque pipeline PCA supplémentaire à l'intérieur d'une instance de la PCA, vous devez retirer un au nombre maximum d'instances de la PCA, comme indiqué dans la formule précédente.

Remarque : Ne comptez pas les processeurs virtuels dotés de la technologie Hyper-Threading comme des noyaux disponibles. Le traitement avec la technologie Hyper-threading fournit une amélioration de la performance faible en comparaison au traitement de la PCA qui sollicite très fortement le processeur et ne doit pas être pris en compte pour l'utilisation prévue.

La limite ci-dessus part du principe que chaque coeur PCA utilise plus de 60% de sa capacité. Si les coeurs utilisent un pourcentage considérablement plus faible de leur capacité, vous pouvez augmenter le nombre d'instances de la PCA au-dessus de cette limite.

Si vous utilisez une carte accélératrice, vous pouvez augmenter ce nombre maximum puisque l'impact est déchargé sur le matériel de la carte.

Remarque : Si vous déchargez le chiffrement sur une carte accélératrice SSL, vous pouvez avoir besoin d'un plus grand nombre d'instances pour capturer et traiter la charge de trafic avec efficacité.

- Voir «Cartes accélératrices prises en charge», à la page 18.

Segmentation du trafic sur plusieurs instances de la PCA

Vous pouvez ajouter des instances de la PCA avec la console Web de la PCA. La PCA prend en charge plusieurs méthodes de segmentation du trafic :

Pour les instances PCA sans équilibrage de charge transparent :

- Filtrage des adresses IP et de port de l'hôte du serveur Web : la méthode la plus utilisée pour la segmentation du trafic par une instance de la PCA est d'effectuer un filtrage des adresses IP et de port de l'hôte du serveur Web.
- Filtrage par segmentation du port du client TCP : la segmentation du port du client TCP peut être utilisée lorsque le trafic de capture se présente comme une seule adresse IP virtuelle (VIP).

Remarque : Les instances de la PCA sont sensibles aux adresses IP et de port. N'ajoutez pas d'instances de la PCA si vous n'avez pas assez d'adresses IP ou de ports pour séparer votre trafic de capture.

Remarque : Si la séparation par adresse IP/de port n'est pas activée dans votre environnement à plusieurs processeurs, vous pouvez au moins créer deux instances de la PCA. La première instance gère le trafic non SSL sur le port 80 tandis que la deuxième gère les transactions SSL sur le port 443. Cette configuration n’exploite pas les cartes accélératrices SSL.

Voici quelques options :

- Déplacez le point de capture derrière l'un des systèmes d'équilibrage de charge.
- Utilisez les adresses IP côté client pour répartir le trafic sur plusieurs instances. Si vous possédez un nombre raisonnable d'adresses IP converties, vous pouvez regrouper les adresses entrantes en blocs de masques de réseau ou en blocs discrètement basés sur les adresses IP pour fournir le trafic au gestionnaire approprié.

Pour les instances PCA avec équilibrage de charge transparent :

Lorsque le mode d'équilibrage de charge transparent est activé, le processus de détermination de la méthode de segmentation du trafic de capture du réseau n'est plus requis. Le trafic de capture du réseau est automatiquement segmenté et

réparti pour créer un environnement doté de l'équilibrage de charge transparent. Le mode d'équilibrage de charge transparent ne nécessite pas autant de configuration de votre interface réseau que le mode sans équilibrage de charge transparent.

Pour plus d'informations sur l'ajout d'instances de la PCA, voir «Console Web de la PCA - Onglet Interface», à la page 71.

Modifications effectuées sur le serveur de la PCA

Lorsque le pack RPM est installé, la PCA est installée par défaut dans `/usr/local/ctccap`. En plus du répertoire d'installation, d'autres modifications sont effectuées sur le système.

Le pack crée le répertoire de fichiers journaux par défaut dans `/var/log/tealeaf` si celui-ci n'existe pas déjà.

- Dans les versions antérieures de la PCA, le répertoire de journaux était `/usr/local/ctccap/logs`.
- Lorsque vous effectuez une mise à niveau à partir d'une version antérieure contenant un répertoire `/usr/local/ctccap/logs` qui n'est pas vide, le pack utilise le répertoire existant au lieu du nouveau répertoire `/var/log/tealeaf`. Ce comportement a pour objectif d'éviter de surprendre l'utilisateur en laissant les anciens fichiers journaux dans l'ancien répertoire (`/usr/local/ctccap/logs`) tout en écrivant les nouveaux dans le nouveau répertoire (`/var/log/tealeaf`) par défaut.

  Remarque : Cette recherche du répertoire `/usr/local/ctccap/logs` est indépendante du préfixe d'installation choisi pour l'installation lors de la mise à niveau. Si vous installez Passive Capture dans `/opt/tealeaf`, le pack recherche toujours un répertoire `/usr/local/ctccap/logs` qui ne soit pas vide.

Les fichiers tealeaf-pca sont inutilisés pour l'instant et réservés pour une utilisation future. Les fichiers tealeaf-web sont utilisés par le fichier `httpd.conf` par défaut pour la console Web. Les fichiers tealeaf-tts sont fournis pour faciliter la configuration des connexions SSL avec le service de transport TeaLeaf. Il est normalement possible pour l'utilisateur racine et celui qui effectue les captures d'écrire dans le répertoire `/usr/local/ctccap/etc`, `ctccap`.

- Installez le fichier crontab : `/etc/cron.d/tealeaf`. Le fichier crontab organise l'exécution de "tealeaf cron" en tant qu'utilisateur racine.
- Installez les scripts d'initialisation suivants dans `/etc/init.d` :
  - `tealeaf-pca`
  - `tealeaf-startup`
- Créez le fichier `capture.log` dans le répertoire de fichiers journaux si celui-ci n'existe pas déjà.

Le pack effectue les actions suivantes afin de modifier les répertoires et les fichiers à l'extérieur du préfixe d'installation.

- Créez le groupe ctccap s'il n'existe pas déjà.
- Créez l'utilisateur ctccap s'il n'existe pas déjà.
- Paramétrez `/usr/local/ctccap/bin/listend` et `/usr/local/ctccap/bin-debug/listend` en tant que bit ID d'utilisateur racine (obligatoire pour que listend puisse ouvrir les périphériques eth pour le reniflement de paquets ; passez ensuite en utilisateur ctccap après avoir ouvert les périphériques eth).

- Supprimez les fichiers de la session PHP dans `/tmp` ; ceux-ci sont considérés comme des fichiers de la session PHP pour la console Web de Passive Capture.
- Mettez à jour `/etc/syslog.conf` (si nécessaire) pour vous assurer qu'il contient une entrée pour la fonction local0 dans le fichier `capture.log` du répertoire de fichiers journaux.
- Redémarrez syslogd afin de le forcer à recharger sa configuration et à utiliser toutes les modifications apportées au fichier `/etc/syslog.conf`.
- Ajoutez le fichier `/etc/ld.so.conf.d/tealeaf.conf` ou modifiez `/etc/ld.so.conf` pour qu'il pointe vers `/usr/local/ctccap/lib` afin de vous assurer que les bibliothèques partagées sont correctement liées pendant l'exécution.

Installation des packs

Le nom de fichier du pack de Tealeaf Passive Capture ressemble au suivant :

```
tealeaf-pca-<nnnn>-<rrr>.<distro>.i386.rpm
```

Où :

- `<nnnn>` représente le numéro de version de génération ; par exemple, 3650.
- `<rrr>` représente le numéro de version RPM. Il s'agit en général d'un numéro à un seul chiffre.
- `<distro>` est un identificateur pour la distribution Linux, comme "RHEL*n*" pour l'édition Red Hat Enterprise Linux *n*.

Vous pouvez accéder au package d'installation d'IBM Tealeaf Application de capture passive CX via IBM Passport Advantage Online.

Copie du pack d'installation à partir du CD-ROM

1. Insérez le CD-ROM dans le lecteur prévu à cet effet.
2. Saisissez les commandes suivantes, en remplaçant `<nnnn>`, `<rrr>` et `<distro>` par les nombres appropriés pour le fichier de pack :

```
mount /mnt/cdrom
cp /mnt/cdrom/tealeaf-pca-<nnnn>-<rrr>.<distro>.i386.rpm /root
umount /mnt/cdrom
```

3. Ejectez le CD-ROM.

Installation du RPM tealeaf-pca

Remarque : L'installation doit être exécutée par un utilisateur racine. Voir Chapitre 9, «Configuration matérielle et installation du système d'exploitation», à la page 235.

Pour installer le pack tealeaf-pca, exécutez la commande suivante.

```
rpm -ivh tealeaf-pca-<nnnn>-<rrr>.<distro>.i386.rpm
```

Où :

- `<nnnn>` représente le numéro de version de génération ; par exemple, 3650.
- `<rrr>` représente le numéro de version RPM. Il s'agit en général d'un numéro à un seul chiffre.
- `<distro>` est un identificateur pour la distribution Linux, comme "RHEL*n*" pour l'édition Red Hat Enterprise Linux *n*.

Vous pouvez également utiliser le gestionnaire de module Yum Update pour installer le pack tealeaf-pca en exécutant la commande suivante :

```
yum install tealeaf-pca-<nnnn>-<rrr>.<distro>.i386.rpm
```

Le logiciel CX PCA est installé par défaut dans `/usr/local/ctccap`.

Vous pouvez définir pour le pack tealeaf-pca un autre répertoire que celui par défaut, à savoir `/usr/local/ctccap`. Vous pouvez définir l'autre répertoire à l'aide des options de commandes `--prefix` ainsi qu'avec les commandes d'installation et de mise à niveau.

Vous trouverez ci-après quelques exemples de commande RPM.

```
rpm -i --prefix=/opt/tealeaf tealeaf-pca-<nnnn>-<rrr>.<distro>.i386.rpm
rpm -U --prefix=/home/tealeaf tealeaf-pca-<nnnn>-<rrr>.<distro>.i386.rpm
```

Où :

- `<nnnn>` représente le numéro de version de génération ; par exemple, 3650.
- `<rrr>` représente le numéro de version RPM. Il s'agit en général d'un numéro à un seul chiffre.
- `<distro>` est un identificateur pour la distribution Linux, comme "RHEL*n*" pour l'édition Red Hat Enterprise Linux *n*.

Si vous n'utilisez pas l'option `--prefix` pendant une installation ou une mise à niveau, le RPM utilise le répertoire d'installation par défaut défini dans le fichier du pack tealeaf-pca, à savoir `/usr/local/ctccap`. Une fois que vous avez changé un pack d'emplacement, vous devez constamment définir l'autre répertoire pour que le pack puisse chercher efficacement les installations précédentes et qu'il puisse les mettre à jour.

Exécution de la PCA pour la première fois en tant qu'utilisateur racine

La première fois que vous exécutez la PCA, vous devez le faire en tant qu'utilisateur `racine`.

Installation du produit Packet Forwarder

IBM Tealeaf Packet Forwarder sert à transférer le trafic Web transmis entre un client et un serveur Web basé sur le Cloud vers un CX PCA basé sur le Cloud.

Le IBM Tealeaf Packet Forwarder est conditionné avec le logiciel IBM Tealeaf CX PCA et partage les mêmes exigences que le logiciel IBM Tealeaf CX PCA. Pour une présentation de Packet Forwarder, voir «Présentation de Packet Forwarder», à la page 6.

CInstallation basée sur le Cloud avec un serveur proxy inversé

Si votre solution Web basée sur le Cloudcomprend un serveur proxy inversé, vous pouvez installer le logiciel Packet Forwarder sur le serveur proxy inversé et sur le serveur CX PCA. Une fois le logiciel Packet Forwarder installé, vous devez configurer l'instance de émetteur Packet Forwarder sur le serveur proxy inverse et les instances de destinataire Packet Forwarder sur le CX PCA.

Installation basée sur le Cloud sans serveur proxy inverse

Si votre solution Web basée sur le Cloud n'inclut pas de serveur proxy inverse, vous pouvez installer le logiciel Packet Forwarder sur chaque serveur Web de votre environnement basé sur le Cloud et sur le serveur CX PCA. Une fois le logiciel Packet Forwarder installé, vous devez configurer les instances d'émetteur Packet Forwarder sur vos serveurs Web et les instances de destinataire Packet Forwarder sur le CX PCA. Chaque instance d'émetteur nécessite une instance de destinataire dédiée. Pour plus d'informations, voir «Configuration d'un Packet Forwarder pour communiquer avec le logiciel CX PCA», à la page 189 and «Configuration d'un destinataire Packet Forwarder et du logiciel CX PCA pour recevoir des paquets transférés», à la page 191.

Exécutez la commande suivante pour installer le package `tealeaf-pktfwdr`.

- Si vous utilisez Red Hat Package Manager, entrez ce qui suit :

  ```
  rpm -ivh tealeaf-pktfwdr-<nnnn>-<rrr>.<distro>.i686.rpm
  rpm -ivh --prefix=/opt/tealeaf tealeaf-pktfwdr-<nnnn>-<rrr>.<distro>.i686.rpm
  ```

  Où :
  - `<nnnn>` représente le numéro de version de génération ; par exemple, 3650.
  - `<rrr>` représente le numéro de version RPM. Il s'agit en général d'un numéro à un seul chiffre.
  - `<distro>` est un identificateur pour la distribution Linux, comme "RHEL*n*" pour l'édition Red Hat Enterprise Linux *n*.
- Si vous utilisez Yellowdog Updater Modified (Yum), entrez ce qui suit :

  ```
  yum install tealeaf-pktfwdr-<nnnn>-<rrr>.<distro>.i686.rpm
  yum install --prefix=/opt/tealeaf tealeaf-pktfwdr-<nnnn>-<rrr>.<distro>.i686.rpm
  ```

  Où :
  - `<nnnn>` représente le numéro de version de génération ; par exemple, 3650.
  - `<rrr>` représente le numéro de version RPM. Il s'agit en général d'un numéro à un seul chiffre.
  - `<distro>` est un identificateur pour la distribution Linux, comme "RHEL*n*" pour l'édition Red Hat Enterprise Linux *n*.

Le logiciel PCA est installé par défaut dans `/usr/local/ctccap`.

Vous pouvez définir pour le pack tealeaf-pca un autre répertoire que celui par défaut, à savoir `/usr/local/ctccap`. Vous pouvez définir l'autre répertoire à l'aide des options de commandes `--prefix` ainsi qu'avec les commandes d'installation et de mise à niveau.

Vous trouverez ci-après quelques exemples de commande RPM.

```
rpm -i --prefix=/opt/tealeaf tealeaf-pktfwdr-<nnnn>-<rrr>.<distro>.i686.rpm
rpm -U --prefix=/home/tealeaf tealeaf-pktfwdr-<nnnn>-<rrr>.<distro>.i686.rpm
```

Où :

- `<nnnn>` représente le numéro de version de génération ; par exemple, 3650.
- `<rrr>` représente le numéro de version RPM. Il s'agit en général d'un numéro à un seul chiffre.
- `<distro>` est un identificateur pour la distribution Linux, comme "RHEL*n*" pour l'édition Red Hat Enterprise Linux *n*.

Si vous n'utilisez pas l'option `--prefix` pendant une installation ou une mise à niveau, le RPM utilise le répertoire d'installation par défaut défini dans le fichier du pack, à savoir `/usr/local/ctccap`. Si vous déplacez un package, vous devez

vous assurer que vous pouvez toujours spécifier le répertoire alternatif afin que le package peut avec précision pour vérifier et mettre à jour toutes les installations précédentes.

Si un répertoire d'installation personnalisée n'est pas utilisée, la structure de répertoires suivante est créée.

```
/opt/tealeaf/
  /bin/pktfwdr
  /bin/ctcstats
  /etc/fwdr-conf.xml
  /etc/fwdr-conf-defaults.xml
  /sbin/
```

Les fichiers principaux suivants sont installés :

Remarque : Il ne s'agit pas d'une liste complète de tous les fichiers que le programme d'installation copie sur le disque.

Tableau 1. Composants fichiers installés

Nom du fichier	Description
`pktfwdr`	Démon de transmission de paquets Pour démarrer une instance Packet Forwarder, exécutez `/user/local/ctccap/bin/pktfwdr -t` comme utilisateur root.
`ctcstats`	Statistiques/métriques opérationnelles
`fwdr-conf.xml`	Fichier de configuration de réacheminement des paquets
`fwdr-conf-defaults.xml`	Fichier de configuration par défaut

Remarque : Si vous utilisez une version 64-bit bits de Red Hat Enterprise Linux, exécutez l'une des commandes suivantes pour installer les bibliothèques de compatibilité 32-bit bits requises :

```
yum install glibc.i686
yum install zlib.i686
```

ou

```
yum install rpm -ivh --prefix=/opt/tealeaf  tealeaf-pktfwdr-<nnnn>-<rrr>.<distro>.i686_24thApr14.rpm
```

Une fois l'installation terminée, vous devez configurer les instances Packet Forwarder. Pour plus d'informations, voir «Configuration d'un Packet Forwarder pour communiquer avec le logiciel CX PCA», à la page 189.

Commandes de Packet Forwarder

Vous pouvez exécuter l'utilitaire Packet Forwarder avec les options de commande.

Packet Forwarder peut être exécuté avec des options pour démarrer une instance, arrêtez une instance, etc. Par exemple, pour démarrer Packet Forwarder, exécuter `/user/local/ctccap/bin/pktfwdr -t` where `-t` est une option qui ordonne à Packet Forwarder de démarrer le service.

Les options suivantes sont disponibles lorsque vous exécutez Packet Forwarder.

Tableau 2. Commandes Packet Forwarder

Commande	Description
`-c` *<fichier de configuration>*	Remplace le fichier de configuration par défaut et vous donne la possibilité d'utilisation d'un fichier de configuration personnalisé, où *<fichier de configuration>* est le nom du fichier de configuration.
`-D`	Supprimer la veille automatique de l'émetteur.

Tableau 2. Commandes Packet Forwarder (suite)

Commande	Description
`-d`	Option de débogage.
`-e`	Mode d'encapsulation de paquet.
`-f` <*règle de filtre*>	Remplace les règles de filtre spécifiées dans le fichier de configuration.
`-h`	Liste des versions et options.
`-i` <*interface NIC*>	Remplace les paramètres NIC spécifiés dans le fichier de configuration.
`-I` <*numéros_instances*>	Indique le nombre d'instances de l'émetteur à charger, où <*numéros_instances*> est le nombre d'instances que vous souhaitez exécuter.
`-k`	Arrêtez le service et ses instances.
`-l`	Signale si le service est en cours d'exécution.
`-n`	Option de débogage pour un environnement autonome.
`-t`	Démarre le service.

Liste de contrôle après installation

Voici la liste d'éléments à contrôler une fois la PCA installée.

Vérification de l'installation de la PCA

Après avoir terminé l'installation de Tealeaf, vous pouvez approuver celle-ci. La commande suivante permet de lire une liste de fichiers avec les paramètres d'utilisateur, de groupe et d'autorisation attendus et de la comparer avec ce qui a été installé. Si la correspondance échoue, un message d'erreur apparaît avec les valeurs réelles et celles qui étaient attendues.

```
tealeaf ps
```

Si la correspondance réussit, une sortie ressemblant à celle-ci s'affiche :

```
[root@venus ~]# tealeaf ps
  PID TTY          TIME CMD
29939 ?        00:00:00 captured
29940 ?        00:00:00 listend
29941 ?        00:00:00 reassd
29942 ?        00:00:00 tcld
29943 ?        00:00:00 deliverd
29945 ?        00:00:00 pipelined
29964 ?        00:00:00 httpd
29969 ?        00:00:00 httpd
29970 ?        00:00:00 httpd
29971 ?        00:00:00 httpd
29972 ?        00:00:00 httpd
29973 ?        00:00:00 httpd
```

Création de clés SSL

Pour un transport sécurisé, vous pouvez appliquer un certificat signé ou autosigné pour que la PCA puisse l'utiliser. Voir «Création d'un certificat autosigné», à la page 207.

Démarrage de la PCA

Une fois l'installation du RPM de la PCA terminée, le premier démarrage doit être effectué en tant qu'utilisateur `racine`. Le fait d'effectuer cette opération en tant qu'utilisateur racine permet à la PCA de paramétrer plusieurs variables du noyau du système à l'aide de la commande `sysctl`, disponible uniquement pour l'utilisateur `racine`.

Remarque : L'utilisateur`ctccap` est crée sans mot de passe attribué, vous ne pouvez donc pas vous connecter à ce compte par défaut. Les risques concernant la sécurité sont minimes ; l'utilisateur `ctccap` peut seulement démarrer et détenir les processus Tealeaf. Selon les conditions de sécurité de votre entreprise, vous pouvez attribuer un mot de passe à l'utilisateur `ctccap` en vous connectant en tant qu'utilisateur `racine`.

La commande `sysctl` est exécutée par le script `tealeaf` principal. Une fois que vous vous êtes connecté en tant qu'utilisateur `racine`, la commande suivante permet le démarrage d'IBM Tealeaf Application de capture passive CX :

```
tealeaf start
```

Une fois la PCA démarrée pour la première fois, vous pouvez exécuter le script en tant qu'utilisateur autre que `ctccap` toutes les fois suivantes. Pour l'exécuter en tant qu'utilisateur `ctccap` :

1. Arrêtez la PCA à l'aide de la commande :
   ```
   tealeaf stop
   ```
2. Passez en utilisateur `ctccap` :
   ```
   su ctccap
   ```
3. Démarrez la PCA en tant qu'utilisateur `ctccap` :
   ```
   tealeaf start
   ```

Remarque : Une fois la PCA démarrée en tant qu'utilisateur `racine`, vous pouvez aussi redémarrer l'ordinateur de la PCA pour l'exécuter en tant qu'utilisateur `ctccap`.

Configuration initiale de la PCA

Tealeaf propose un ensemble d'étapes de configuration initiale utilisables ou modifiables dans la plupart des environnements de la PCA. Vous devez effectuer la configuration initiale de la PCA dès maintenant.

- Voir «Configuration initiale de la PCA», à la page 45.

Lorsque vous avez fini, retournez à cette page, passez en revue et accomplissez les tâches suivantes.

Vérification des paramètres de connexion autorisée

Pendant l'installation, la PCA paramètre le nombre maximum de connexions autorisées pour chaque instance de la PCA. Par défaut, ces valeurs sont définies sur :

- Nombre maximum de connexions Current : `5000`
- Nombre maximum de connexions SYN/WAIT : `1000`

Remarque : Ces paramètres définissent le nombre maximum de connexions autorisées pour chaque instance de la PCA. Si le nombre réel de connexions dépasse ces valeurs, cela peut entraîner une perte de données. Toute analyse des

performances de la PCA basée sur son état réel peut être dénaturée en fonction du volume de données non capturé. Vous devez passer ces paramètres en revue le plus tôt possible.

Vous pouvez vérifier l'état actuel de ces paramètres dans l'onglet Statistiques de la console Web de la PCA. Pour chaque instance de la PCA, les statistiques à comparer sont les suivantes :

Current
Maximum

`Connexions Current`
`Nombre maximum de connexions Current`

`Nombre de connexions SYN/WAIT`
`Nombre maximum de connexions SYN/WAIT`

Si l'une des valeurs actuelles est proche du nombre maximum qui lui correspond, vous devez envisager d'augmenter le nombre maximum pour toutes les instances PCA affectées. Cela permet de s'assurer que les données sont correctement capturées.

Configuration de la PCA pour la capture d'applications Internet riches

Si votre application Internet riche (RIA) déployée soumet des données à la capture, vous devez vérifier que la PCA est configurée pour capturer tout type de données soumises.

Remarque : Si la PCA n'est pas configurée pour capturer les types POST et Mime soumis par votre application Internet riche, ces hits ne seront pas capturés et les données qu'ils contiennent seront perdues pour Tealeaf. Vérifiez que vous disposez d'une liste de tous les types requis que la PCA doit capturer pour la réexécution des RIA et la création d'un rapport les concernant. Cette liste inclut tout type personnalisé déployé.

Capture de contenu JavaScript

Par défaut, la PCA exclut la capture de fichiers JavaScript. La capture de contenu JavaScript statique par la PCA est rarement nécessaire pour que la réexecution des applications Internet riches soit efficace. Dans la plupart des cas, ces fichiers peuvent être stockés dans une base de données statique ou référencés à nouveau à l'aide des règles de réexécution.

Remarque : Si votre application Web génère du contenu JavaScript dynamique, il est possible de configurer la PCA manuellement pour capturer ces fichiers.

Capture de XML

Par défaut, la PCA capture les types de contenu suivants sans avoir besoin de configuration supplémentaire.

- `application/xml`
- `text/xml`

Les contenus de ces types soumis au serveur Web sont insérés dans la mémoire tampon de la demande dans la section `[xml1]` pour être traités par le système Tealeaf.

Types de capture RIA courants

Les types de capture suivants doivent être ajoutés aux types de capture de la PCA en fonction de l'application contrôlée. Ces types peuvent être définis dans la liste de types de POST XML.

- Voir «A configurer».
- `application/json`
- `application/x-json`
- `text/json`
- `text/x-json`

Dans les sections suivantes, vous allez pouvoir étudier des exemples d'ensembles de types pour différents types d'applications Internet riches.

Exemple de RIA : Ajax

Types capturés par défaut :

- `application/xml`
- `text/xml`
- `application/json`
- `text/json`

Les types personnalisés suivants peuvent être présents et doivent être configurés :

- `ajax/xml`
- Contenus JavaScript générés de façon dynamique

A configurer

Si vous souhaitez que Tealeaf capture d'autres types de POST XML, des configurations supplémentaires seront nécessaires selon le numéro de build de votre logiciel IBM Tealeaf Application de capture passive CX :

- Pour les versions 3326 et ultérieures : vous devez ajouter le type de POST XML à la liste blanche qui se trouve dans l'onglet Pipeline de la console Web de la PCA. Voir «Console Web de la PCA - Onglet Pipeline», à la page 101.
- Build 3325 ou antérieure : contactez http://support.tealeaf.com.

Service Tealeaf Passive Capture

Le pack de Tealeaf Passive Capture est maintenant installé. Vous pouvez utiliser les commandes du service pour redémarrer, démarrer et arrêter le logiciel Tealeaf Passive Capture. En voici quelques exemples.

```
tealeaf restart
tealeaf start
tealeaf stop
```

Si certains des composants de Passive Capture ne s'interrompent pas à temps, la commande `tealeaf restart` ne pourra pas les démarrer correctement après que vous essayez de les arrêter. Utilisez donc plutôt la commande `tealeaf stop` pour vérifier que le logiciel Tealeaf Passive Capture a bien été arrêté.

Pour déterminer si certains processus de Tealeaf sont toujours en cours d'exécution, utilisez la commande suivante : ps Uctccap

Correctifs CX PCA

Des correctifs sont publiés pour améliorer les performances et la fiabilité du logiciel CX PCA.

Une fois que votre serveur CX PCA a été installé et configuré, vous pouvez appliquer des correctifs disponibles pour votre version du logiciel CX PCA. Les correctifs de CX PCA peuvent être téléchargés à partir d'IBM Fix Central, à l'adresse http://www.ibm.com/support/fixcentral/. Pour rechercher des correctifs à partir de la page Fix Central :

1. A l'aide de votre navigateur Web, accédez à http://www.ibm.com/support/fixcentral/.
2. Recherchez **Groupe de produits**, puis sélectionnez **Enterprise Marketing Management**.
3. Recherchez **Sélection dans Enterprise Marketing Management**, puis sélectionnez **Tealeaf Customer Experience**.
4. Cliquez sur **Continuer**.
5. Dans le menu Identifier des correctifs, sélectionnez **Rechercher des correctifs**, puis cliquez sur **Continuer** pour afficher tous les correctifs Tealeaf disponibles. Vous pouvez utiliser la section Filtrer votre contenu pour filtrer la liste des correctifs disponibles.

Assurez-vous de bien télécharger le correctif approprié pour votre système d'exploitation.

Traitement des incidents et conseils

Dans cette section, vous pourrez découvrir comment identifier et résoudre les problèmes sur la PCA.

Fichiers CORE

La présence de fichiers `core.*` dans le répertoire `/usr/local/ctccap` indique que la capture a échoué et qu'un rapport a été rédigé sous la forme d'un fichier de vidage CORE.

Retards au démarrage

Si le fichier `/etc/resolv.conf` contient des informations inexactes sur le réseau local, des retards peuvent survenir durant la procédure de démarrage et lors de l'exécution de diverses commandes relatives au réseau. Les retards peuvent se manifester sous la forme d'une tentative de connexion en SSH lente lorsque le délai d'attente est dépassé pour le démon SSH sur le poste de travail hôte de Passive Capture car vous utilisez les informations inexactes sur la résolution DNS qui se trouvent dans le fichier `/etc/resolv.conf`.

Ce fichier peut contenir des informations incorrectes s'il provient d'une configuration IP statique sur un réseau différent. Il peut aussi provenir de l'arrêt du poste de travail à l'aide du protocole DHCP bien que le démarrage avec DHCP crée en général un fichier `/etc/resolv.conf`. En fonction de la configuration du poste de travail pour le protocole DHCP ou pour une adresse IP statique, le processus de réparation du fichier sera différent.

DHCP

Si le logiciel Passive Capture a été configuré pour le DHCP, suivez alors les instructions suivantes :

1. Connectez-vous en tant qu'utilisateur racine.
2. Supprimez le fichier `/etc/resolv.conf`.
3. Exécutez `shutdown now` pour passer en mode utilisateur unique.
4. Utilisez la commande `exit` pour quitter le mode utilisateur unique et permettre au système de créer un nouveau fichier `/etc/resolv.conf`.

IP statique

Si Passive Capture a été configuré avec une adresse IP statique, suivez alors les instructions suivantes :

1. Connectez-vous en tant qu'utilisateur racine.
2. Supprimez le fichier `/etc/resolv.conf`.
3. Exécutez `tealeaf ipconfig` pour accéder à nouveau aux informations DNS puis quittez.
4. Le programme créé un nouveau fichier `/etc/resolv.conf`, qui prend effet immédiatement.

Mode utilisateur unique

Si vous venez de redémarrer ou de mettre sous tension la machine hôte de Passive Capture et que vous devez passer en mode utilisateur unique, suivez alors les instructions suivantes tout en utilisant le chargeur de démarrage GRUB :

1. Lorsque le menu de démarrage de GRUB s'affiche, appuyez sur la barre d'`espace` pour empêcher tout démarrage automatique.
2. Utilisez les touches de déplacement pour sélectionner le noyau et la version de Red Hat Enterprise Linux que vous souhaitez démarrer.
3. Appuyez sur la touche `A` pour ajouter les options du noyau.
4. Sur l'invite d'ajout `grub`, ajoutez le mot `single`. Appuyez sur la barre d'`espace` puis saisissez `unique`.
5. Appuyez sur la touche `entrée` pour accepter la nouvelle valeur puis démarrez.
6. Pour plus d'informations, voir le chapitre sur la reprise du système de base dans le guide d'administration du système Red Hat Enterprise Linux.

Accès aux journaux de capture

L'examen des journaux de Passive Capture permet de repérer les problèmes éventuels. Si Capture ne démarre pas, `capture.log` affiche en général la raison de l'échec du démarrage, comme par exemple une erreur de syntaxe ou encore une entrée incorrecte dans le fichier de configuration.

Un autre journal consignant le traitement des incidents, `maintenance_200xxxxx.log`, affiche les mauvaises conditions qui forcent le redémarrage et/ou l'arrêt de Passive Capture.

Il est possible d'accéder à ces deux journaux via la console Web ou un éditeur de texte de Linux, dans le répertoire de journaux par défaut de Passive Capture. Selon la version de Passive Capture, ils peuvent se trouver dans `/usr/local/ctccap/logs` ou dans `/var/log/tealeaf`.

Remarques relatives à la mise à niveau de la PCA

Vous trouverez ici les différents éléments à prendre en compte avant la mise à niveau de votre version.

Avant la mise à niveau

Cette section présente les opérations à effectuer avant une mise à niveau.

Si vous effectuez une mise à niveau vers un système d'exploitation 64 bits

Si vous passez d'une version 32 bits à une version 64 bits d'un système d'exploitation pris en charge, vous devez installer un ensemble de bibliothèques 32 bits pour la prise en charge de la PCA, qui est une application 32 bits.

- Voir «Packs nécessaires», à la page 20.

Avant l'activation du mode d'équilibrage de charge transparent (TLB)

La fonction d'équilibrage de charge transparent est disponible dans la Build 3620 ou ultérieure de la PCA. Si vous effectuez une mise à niveau à partir d'une build PCA antérieure à la 3620, vous pouvez activer l'équilibrage de charge transparent sur votre PCA.

Remarque : Si vous activez l'équilibrage de charge transparent pour votre communication réseau, les paramètres d'interface réseau précédents sont écrasés. Avant d'activer l'équilibrage de charge transparent, veillez à copier les paramètres d'interface réseau existants si vous désactivez le mode TLB.

Pour plus d'informations sur l'équilibrage de charge transparent, voir «Présentation de l'équilibrage de charge transparent de d'CX PCA», à la page 8.

Validation des clés SSL actuelles

Avant la mise à niveau, vous voudrez probablement faire un test pour savoir si vos clés SSL actuelles sont toujours valides dans la nouvelle build de la PCA. Les étapes suivantes permettent d'indiquer comment extraire le processus reassd de la nouvelle distribution de la PCA et la commande appropriée pour l'exécuter.

1. Obtenez la dernière build de la PCA. Pour plus d'informations sur le téléchargement d'IBM Tealeaf , reportez-vous à IBM Passport Advantage Online.
2. Copiez le RPM dans la PCA dans le répertoire `/tmp`.
3. Exécutez la commande suivante pour extraire le processus reassd du RPM fourni et pour le placer dans le répertoire suivant :

   ```
   rpm2cpio tealeaf-pca-<nnnn>-<rrr>.<distro>.i686.rpm | cpio \
     -ivd./usr/local/ctccap/bin-debug/reassd ; \
     mv usr/local/ctccap/bin-debug/reassd .
   ```

   Où :

   - `<nnnn>` représente le numéro de version de génération ; par exemple, 3650.
   - `<rrr>` représente le numéro de version RPM. Il s'agit en général d'un numéro à un seul chiffre.
   - `<distro>` est un identificateur pour la distribution Linux, comme "RHEL*n*" pour l'édition Red Hat Enterprise Linux *n*.
4. Le processus reassd doit se trouver dans le répertoire `/tmp`.
5. Pour tester vos clés SSL actuelles, exécutez la commande suivante à partir du répertoire `/tmp` :

   ```
   ./reassd -j
   ```

   a. Si les clés SSL actuelles sont correctement chargées, le message suivant s'affiche alors :

```
Success loading configuration and SSL keys.
```

b. Si la commande ne parvient pas à charger les clés SSL actuelles, le message suivant s'affiche alors :

```
Failed loading configuration (1), likely due to:

    * Loading bad SSL keys
    * Error in configuration file
    * Other unknown error
```

Si le chargement échoue, le fichier `capture.log` de la PCA enregistre alors le message d'erreur suivant indiquant le chargement de mauvaises clés SSL :

```
Couldn't create reveal object: 1
```

Pour plus d'informations sur le processus de recréation des clés SSL, voir "Traitement des incidents - Capture" dans le manuel de dépannage d'*IBM Tealeaf*.

Mise à niveau basique

Remarque : La mise à niveau doit être effectuée par un utilisateur racine. Voir Chapitre 9, «Configuration matérielle et installation du système d'exploitation», à la page 235.

Vous pouvez utiliser une seule commande de Linux pour exécuter la mise à niveau si votre installation PCA respecte les conditions suivantes :

- Les paramètres de configuration de la PCA sont stockés dans le répertoire par défaut : `/usr/local/ctccap/etc`.
- Si vous effectuez une mise à niveau depuis une édition 31xx et que l'authentification d'utilisateur est employée, voir «Mise à niveau de la PCA avec une authentification d'utilisateur». Dans les autres cas, procédez comme suit.

Si votre installation respecte les conditions ci-dessus, voici comment procéder pour la mise à niveau

1. Effectuez une copie de sauvegarde de `/usr/local/ctccap/etc` :

```
mkdir /root/tmp
cp -r /usr/local/ctccap/etc /root/tmp
```

2. Vous pouvez exécuter une mise à niveau basique à l'aide de la commande suivante :

```
rpm -Uvh tealeaf-pca-XXXX-1.RHEL6.i686.rpm
```

où *XXXX* représente le numéro de version de la CX PCA. Par exemple, si vous effectuez une mise à niveau vers CX PCA version 3620, exécutez

```
rpm -Uvh tealeaf-pca-3620-1.RHEL6.i686.rpm
```

.

Mise à niveau de la PCA avec une authentification d'utilisateur

Si votre PCA opère au sein d'un environnement Tealeaf dans lequel l'authentification d'utilisateur est activée, le processus de mise à niveau peut nécessiter des étapes supplémentaires.

Pour les versions de la PCA antérieures à 3200, des modifications majeures ont été implémentées dans la manière de configurer l'authentification d'utilisateur. La mise

à niveau d'une build 31xx de la PCA vers une build 32xx ou 33xx est plus complexe si l'authentification d'utilisateur est activée. Pour la mise à niveau, vous devez suivre les instructions suivantes :

1. Faites une copie de /usr/local/ctccap/etc :

```
mkdir /root/tmp
cp -r /usr/local/ctccap/etc /root/tmp
```

2. Supprimez le pack tealeaf-pca existant. Supprimez les fichiers restants dans /usr/local/ctccap :

```
rpm -e tealeaf-pca
cd /usr/local/ctccap
rm -rf *
```

   Remarque : Vérifiez que vous êtes dans le bon répertoire avant d'exécuter la commande rm.

3. Installez le nouveau pack PCA :

```
rpm -ivh tealeaf-pca-3315.rpm
```

4. Copiez les fichiers ctc-conf.xml, privacy.cfg et tous les fichiers *.ptl originaux dans /usr/local/ctccap/etc. Si on vous invite à le faire, écrasez les fichiers actuels :

```
cd /root/tmp/etc
cp ctc-conf.xml privacy.cfg *.ptl /usr/local/ctccap/etc
```

5. Copiez le fichier httpd.users dans /usr/local/ctccap/etc et tealeaf-web.users :

```
cp httpd.users /usr/local/ctccap/etc
cd /usr/local/ctccap/etc
cp httpd.users tealeaf-web.users
```

6. Modifiez /usr/local/ctccap/etc/runtime.conf, et ajoutez à la fin de celui-ci les lignes suivantes :

```
httpd_userauth_enable="YES"
httpd_userauth_realm="Tealeaf PCAv2"
httpd_userauth_require="valid-user"
httpd_userauth_type="Basic"
```

7. Démarrez httpd.

```
tealeaf start all
```

8. Vérifiez que la console Web est en cours d'exécution et que l'authentification d'utilisateur est toujours activée. Vérifiez que le processus de capture est en cours d'exécution.
9. La mise à niveau est terminée.

Configuration de nouveaux types de données

Si vous avez effectué une mise à niveau à partir d'une build de la PCA antérieure à 3324, vous devez passer en revue et configurer les types de données capturés par IBM Tealeaf Application de capture passive CX afin de vérifier que le logiciel capture les types de données souhaités. Pour les build antérieures à 3324, certains de ces types de données n'étaient pas disponibles à la capture ou n'étaient pas configurés pour la capture par défaut.

Remarque : Si vous mettez votre PCA à niveau en y incluant une application Internet riche, vous devez configurer les types de POST XML. Voir «Configuration de la PCA pour la capture d'applications Internet riches», à la page 31.

Pour plus d'informations sur la configuration des types de POST XML, voir «Console Web de la PCA - Onglet Pipeline», à la page 101.

Désinstallation ou annulation du logiciel Application de capture passive CX

Vous pouvez suivre les instructions suivantes pour désinstaller la PCA si nécessaire.

Désinstallation du logiciel Application de capture passive CX

Pour procéder à la désinstallation :

Arrêtez la PCA de Tealeaf. Dans la ligne de commande, saisissez :

```
tealeaf stop
```

Dans l'invite de commande UNIX, vérifiez tous les processus en cours d'exécution. Une fois connecté en tant qu'utilisateur racine, saisissez la commande suivante :

```
PS Tealeaf
```

Si ne serait-ce qu'un processus est en cours d'exécution, saisissez la commande suivante :

```
killall <processname>
```

Où `<processname>` correspond au nom du processus en cours.

Sauvegardez le dossier `ctccap/etc` existant. Ce dossier contient vos fichiers de configuration personnalisée tels que `ctc-conf.xml`, des clés PTL stockées et bien plus. Pour désinstaller le logiciel, exécutez la commande suivante :

Remarque : Cette commande retire le logiciel PCA du serveur Linux.

```
rpm -e tealeaf-pca
```

La PCA est désinstallée. Pour que la désinstallation soit totale, supprimez aussi le dossier `/usr/local/ctccap`.

Revenez à la version antérieure de Application de capture passive CX

Pour revenir à une version précédente :

1. Suivez les instructions de désinstallation.

   Remarque : Avant de procéder à l'installation, vérifiez que le dossier `/usr/local/ctccap` n'existe pas déjà.
2. Installez le pack RPM de la version précédente. Voir «Installation du RPM tealeaf-pca», à la page 25.
3. Restaurez la version des fichiers de configuration que vous avez sauvegardée dans le dossier `ctccap/etc`.

Désinstallation du logiciel Packet Forwarder

Vous pouvez suivre les instructions suivantes pour désinstaller Packet Forwarder si nécessaire.

Vous pouvez utiliser Red Hat Package Manager (RPM) pour désinstaller le Packet Forwarder. Pour désinstaller l' Packet Forwarder, entrez la commande suivante à partir d'une ligne de commande :

```
rpm -ev tealeaf-pktfwdr-<nnnn>-<rrr>.<distro>.i686
```

où :

- `<nnnn>` représente le numéro de version de génération ; par exemple, 3650
- `<rrr>` correspond au numéro de révision RPM ; par exemple, 1
- `<distro>` est un identificateur pour la distribution Linux, comme "RHEL6" pour Red Hat Enterprise Linux 6

Chapitre 3. Configuration de CX PCA

Il est possible de configurer IBM Tealeaf Application de capture passive CX à l'aide d'une console Web ou des fichiers de configuration stockés sur le serveur de la PCA. Cette section indique comment configurer la PCA et les étapes spécifiques à chaque mécanisme.

Présentation de la configuration de Passive Capture

Vous pouvez configurer le logiciel Passive Capture par le biais de la console Web de Passive Capture ou en modifiant directement le fichier de configuration (`ctc-conf.xml`) à l'aide de l'éditeur vi.

Remarque : pour la majorité des activités, il est conseillé de configurer la PCA à partir de la console Web. Configurez la PCA via le fichier `ctc-conf.xml` uniquement si le paramètre requis n'est pas disponible à partir de la console Web.

Configuration à l'aide de la console Web

La console Web de la PCA propose une interface graphique pratique pour contrôler et configurer IBM Tealeaf Application de capture passive CX ainsi que ses connexions.

Remarque : tous les paramètres de configuration nécessaires à l'initialisation d'IBM Tealeaf Application de capture passive CX sont disponibles à partir de la console Web.

Remarque : La console Web Application de capture passive CX ne prend pas en charge la saisi des caractère multi-octets dans une zone. Si vous souhaitez configurer un paramètre avec des caractères multi-octets, vous devez éditer la configuration. Pour plus d'informations sur l'édition du fichier de configuration, voir «Configuration à l'aide de `ctc-conf.xml`».

- Voir «Navigateurs pris en charge pour la console Web de la PCA», à la page 54.

Configuration à l'aide de `ctc-conf.xml`

Même si toutes les options de configuration sont disponibles par le biais de la console Web, utilisez l'éditeur vi pour visualiser et modifier la totalité des zones de configuration, lorsque cela est nécessaire.

- Voir «Fichier de configuration Passive Capture `ctc-conf.xml`», à la page 171.

Configuration à l'aide de `runtime.conf`

Les paramètres de configuration relatifs à IBM Tealeaf Application de capture passive CX sont disponibles par le biais de la console Web de la PCA ou de `ctc-conf.xml` si nécessaire.

Les paramètres de configuration concernant l'interaction entre la PCA et le système d'exploitation sont spécifiés dans deux fichiers situés dans le répertoire suivant :

`/usr/local/ctccap/etc/`

Fichiers

- `tealeaf.conf` : ce fichier contient les paramètres et les valeurs par défaut pour la configuration au niveau du système d'exploitation.

  Remarque : le fichier `tealeaf.conf` doit posséder une autorisation en lecture seule pour tous les utilisateurs, car il ne doit jamais être modifié.
- `runtime.conf` : utilisez ce fichier pour redéfinir les valeurs des paramètres répertoriés dans `tealeaf.conf`.

Pour modifier un paramètre de fonctionnement :

1. Copiez l'entrée du fichier `tealeaf.conf`.
2. Collez-la dans le fichier `runtime.conf` et modifiez la valeur du paramètre.
3. Enregistrez le fichier `runtime.conf` et redémarrez la PCA.

Enregistrement des modifications

Remarque : après avoir enregistré les modifications dans l'onglet **Interface** de la console Web, redémarrez manuellement la PCA. Les modifications effectuées dans les autres onglets de la console Web ne nécessitent pas de redémarrer manuellement la PCA.

- Il est nécessaire de redémarrer lorsque les modifications ont été effectuées à partir du fichier ctc-conf.xml.

Voir «Console Web de la PCA - Onglet Console», à la page 70.

Déchiffrement SSL

Chargez le déchiffrement SSL par le biais de l'IU Web ou à l'aide de la ligne de commande si vous devez déchiffrer vos données Web.

A. IU Web :

1. Rendez-vous sur `https://<machineIP>:8443/` et cliquez sur **Clés SSL**.
2. Cliquez sur **Chargées** en haut de la page pour afficher les clés SSL chargées et en ajouter de nouvelles.
3. Lorsque vous avez terminé, cliquez sur **Enregistrer**.
   - Pour plus d'informations sur l'utilisation de la console Web du logiciel Passive Capture, voir «Navigateurs pris en charge pour la console Web de la PCA», à la page 54.

B. Ligne de commande :

1. Modifiez le fichier `/usr/local/ctccap/etc/ctc-conf.xml`.
2. Modifiez le noeud XML CaptureKeys.
3. Modifiez les options restantes à l'aide de l'IU Web ou du fichier `/usr/local/ctccap/etc/ctc-conf.xml`.

C. Redémarrage des services :

- Lorsque vous effectuez des modifications à l'aide de la console Web, les services redémarrent automatiquement pour qu'elles soient appliquées.
- Si vous avez modifié le fichier `ctc-conf.xml`, redémarrez manuellement les services de capture à l'aide des commandes suivantes :

```
tealeaf stop capture
tealeaf start capture
```

- Si vous n'utilisez pas Tealeaf Cookie Injector pour la mise en sessions, configurez les paramètres de mise en sessions dans l'agent de session TLSessioning dans le fichier `TealeafCaptureSocket.cfg` sur le serveur IBM Tealeaf CX. Voir section "Agent de session de mise en sessions" du *Manuel de configuration d'IBM Tealeaf CX*.

Référence de la ligne de commande de la PCA Tealeaf

Cette section contient l'ensemble des commandes, des actions et des options pouvant être exécutées à l'aide de la commande de script `tealeaf`. Cette dernière est essentiellement utilisée pour la post-installation des tâches suivantes :

- certaines fonctions d'administration et de maintenance ;
- certains accès aux fonctions de la console Web lorsque l'interface n'est pas disponible ;
- opérations de débogage.

Commande de base

```
tealeaf [options] action [service ...]
```

Consultez

- «Options»
- «Actions»
- «Services», à la page 45

Options

Commande
Description

-h Affiche l'aide.

-n Affiche les commandes sans les exécuter.

-v Affiche plus de messages (mode prolixe).

Les options sont transmises au service sauf lorsque vous spécifiez `all` pour le service. Voir «Services», à la page 45.

Actions

Action **Description**

allselfsignedcerts
Permet de générer tous les certificats autosignés lorsqu'il en manque.

bwmon Permet d'exécuter l'utilitaire bwMon.

capturekeys2ptl
Permet de convertir tous les fichiers PEM dans le répertoire capturekeys.

clearstats
Permet d'effacer les statistiques de toutes les instances.

configdiffs
Permet d'afficher les différences entre les fichiers de configuration actuels et par défaut.

deletestats
Permet de supprimer les statistiques de toutes les instances.

disable
Empêche un ou plusieurs services de démarrer.

enable Permet à un ou plusieurs services de démarrer.

env Permet d'afficher l'"environnement tealeaf".

genselfsignedcert
Permet de générer un certificat autosigné.

ifdetails
Permet d'afficher des informations détaillées sur le périphérique réseau défini.

ifstat Permet d'afficher les statistiques concernant le périphérique réseau défini.

ifsummary
Permet d'afficher les informations récapitulatives concernant les périphériques réseau.

ifup Permet d'activer tous les périphériques réseau.

ipconfig
Permet de configurer les périphériques réseau.

maint Permet d'exécuter le script de maintenance.

man Permet d'afficher les pages d'aide fournies.

no Permet de définir une variable de configuration d'exécution sur "NO".

openssl
Permet d'exécuter le logiciel OpenSSL fourni.

pem2ptl
Permet de chiffrer les fichiers PEM au format PTL.

ps Permet d'afficher les processus de capture à l'aide de /bin/ps.

restart
Permet d'arrêter puis de redémarrer le service spécifié.

rolllog
Permet d'assurer l'enregistrement tournant de tous les fichiers journaux ou d'un seul préalablement défini.

showstats
Permet d'afficher les statistiques de capture.

showstatsxml
Permet d'afficher les statistiques de capture en XML.

start Permet de démarrer tous les services ou le service spécifié.

stats Permet d'exécuter l'utilitaire de statistiques.

status Permet d'afficher le statut de la capture et du processus HTTPd.

stop Permet d'arrêter tous les services ou le service spécifié.

tcpdump
Permet d'exécuter le package tcpdump fourni.

testconn
Permet d'exécuter le programme de test de connexion du service de transport TeaLeaf.

top Permet d'afficher les processus de capture à l'aide de /usr/bin/top.

tzconfig
Configurer le fuseau horaire

Remarque : Les paramètres de fuseau horaire doivent être conformes aux fuseaux horaires pris en charge par PHP. Pour obtenir la liste des fuseaux horaires pris en charge, voir http://www.php.net/manual/en/timezones.php .

userauthpw
Permet d'ajouter ou de mettre à jour un mot de passe utilisateur de la console Web.

validate
Permet de valider l'utilisateur, le propriétaire et les autorisations des fichiers de la PCA.

yes Permet de définir une variable de configuration d'exécution sur "YES".

Services

Il est possible de définir les services suivants pour les actions `disable`, `enable`, `start`, `status`, et `stop` :

- `all`
- `capture` : par le biais de `captured`
- `httpd` : par le biais de `httpd`

Exemples de commandes

```
tealeaf ifdetails em0
```

```
tealeaf showstats
```

```
tealeaf start
```

- Lorsque `start` est utilisé comme racine, le script permet d'ouvrir les interfaces de capture principale et secondaire.

```
tealeaf start all
```

- Lorsque `start` est utilisé comme racine, le script permet d'ouvrir les interfaces de capture principale et secondaire.

```
tealeaf stop
```

```
tealeaf start capture
```

```
tealeaf start capture -r
```

Configuration initiale de la PCA

Remarque : cette section fournit un cadre pour la configuration initiale d'un composant du système IBM Tealeaf CX via un modèle de déploiement simplifié. Selon votre solution de déploiement Tealeaf, une configuration supplémentaire peut être nécessaire. Pour toute question concernant la configuration, contactez http://support.tealeaf.com.

Après l'installation du logiciel PCA, vous pouvez suivre les étapes ci-dessous afin de configurer la PCA pour capturer le trafic des applications Web et le transférer vers un ou plusieurs serveurs de traitement.

Prérequis

Avant de commencer à configurer la PCA, assurez-vous de répondre aux exigences suivantes et de posséder ces informations :

1. Le système d'exploitation du serveur de la PCA est installé avec les packs Tealeaf recommandés. Voir Chapitre 9, «Configuration matérielle et installation du système d'exploitation», à la page 235.
2. Le système d'exploitation est correctement configuré. Voir Chapitre 7, «Configuration de Passive Capture sur Red Hat Enterprise Linux (RHEL)», à la page 225.
3. Le logiciel PCA est installé dans un répertoire situé sur le système de la PCA. Voir Chapitre 2, «Installation», à la page 17.
4. Afin de terminer les étapes de cette configuration, vous devez avoir les informations suivantes à portée de main :
   a. l'adresse IP du système de la PCA ;
   b. les cartes d'interface réseau connectées à l'unité de la PCA fournissant la source du trafic ;
   c. le nom d'hôte ou l'adresse IP et le numéro de port du serveur de traitement.
      - Si vous utilisez le Health-Based Routing (HBR), vous devez connaître le nom d'hôte ou l'adresse IP et le numéro de port de la machine HBR. Voir section "Agent de session Health-Based Routing (HBR)" du *Manuel de configuration d'IBM Tealeaf CX*.

Remarque : l'utilisateur ctccap est créé sans mot de passe attribué, vous ne pouvez donc pas vous connecter à ce compte par défaut. Les risques concernant la sécurité sont minimes; l'utilisateur ctccap peut seulement démarrer et détenir les processus Tealeaf. Selon les conditions de sécurité de votre entreprise, vous pouvez attribuer un mot de passe à l'utilisateur ctccap en vous connectant en tant qu'utilisateur racine.

Exemple de configuration

La configuration de la PCA dépend de son environnement de serveur. Cette section contient un exemple de configuration pour un système simple :

- 1 serveur PCA
- 1 instance PCA
- 1 serveur de traitement

Situations complexes

Pour capturer des applications Web plus complexes, il existe de nombreuses architectures de déploiement de PCA. Elles peuvent inclure l'utilisation de plusieurs PCA et instances PCA ainsi que de mécanismes de filtrage. Vous trouverez ci-dessous des exemples de scénarios dans lesquels vous pourriez avoir besoin d'aide pour la configuration de la PCA.

Remarque : Si l'environnement de votre application Web remplit un ou plusieurs des critères suivants, nous vous recommandons de contacter http://support.tealeaf.com ou les services professionnels de Tealeaf avant de commencer la configuration.

1. Applications Web volumineuses. Si vous envoyez plus de 200 hits/s à l'aide du protocole SSL ou plus de 400 hits/s via le protocole HTTP en texte clair :
   - Partagez le trafic entre plusieurs instances PCA.
   - Filtrez les adresses IP des serveurs Web à partir desquels vous souhaitez effectuer des captures. Vous pouvez instaurer le filtrage au niveau de la PCA ou au niveau du réseau. Tealeaf vous recommande la deuxième option ; cela réduit les opérations de traitement sur la PCA.

     Remarque : il est possible de filtrer les adresses IP uniquement lorsqu'elles ne sont pas converties en interne. Pour plus d'informations, contactez votre administrateur de réseau.
2. Capture d'une plage d'adresses IP. Lorsque vous capturez une plage de 25 adresses IP ou plus sur la PCA :
   - Créez des filtres d'adresses IP afin de supprimer du contenu.
   - Utilisez des masques de réseau pour limiter le nombre d'entrées dans votre configuration.
   - Partagez le trafic entre plusieurs instances de la PCA.

Pour plus d'informations, contactez http://support.tealeaf.com.

Etapes de configuration

Les sections suivantes contiennent les étapes de configuration.

Apache : démarrage

Suivez les étapes ci-dessous pour commencer votre configuration :

1. Connectez-vous en tant qu'utilisateur `racine`.
2. Exécutez le script Tealeaf pour lancer le processus Apache :
   ```
   tealeaf start httpd
   ```
3. Pour vous assurer que le processus a correctement démarré, utilisez les commandes suivantes afin de renvoyer les processus Apache en cours d'exécution.
   ```
   tealeaf ps
   tealeaf status
   ```

La sortie de la commande doit indiquer qu'au moins un processus est en cours d'exécution.

- Si le démarrage d'un processus a échoué, consultez les messages d'erreur de démarrage contenus dans le fichier `/var/log/tealeaf/capture.log` afin de déterminer le problème.
- Si la console Web de la PCA (processus HTTPd) ne démarre pas en raison d'un changement de la configuration, vous pouvez modifier manuellement la configuration dans le fichier `/usr/local/ctccap/etc/ctc-conf.xml`. Voir «Fichier de configuration Passive Capture `ctc-conf.xml`», à la page 171.

Ouverture de la console Web de la PCA

Après le démarrage des processus Apache, vous pouvez ouvrir la console Web de la PCA pour consulter la configuration.

- Voir «Navigateurs pris en charge pour la console Web de la PCA», à la page 54.

1. Ouvrir la console Web de la PCA :
   a. Protocole HTTP sécurisé :

`https://<servername>:8443`

b. Protocole HTTP :

`http://<servername>:8080`

2. Si les URL ci-dessus ne fonctionnent pas, modifiez le nom du serveur et le numéro de port avec l'aide de votre administrateur de réseau.

   Remarque : il est peut être nécessaire de vous authentifier pour accéder à la console Web de la PCA.

Configuration de l'interface CX PCA

lorsque le logiciel PCA est installé et est en cours d'exécution, il n'est pas encore en mesure de capturer le trafic bidirectionnel. Après l'installation du logiciel IBM Tealeaf CX PCA, vous devez configurer l'interface réseau pour capturer le trafic bidirectionnel.

Si un équilibreur de charge est déployé entre le CX PCA et le serveur Web ou si plusieurs serveurs Web fonctionnent sous un IP virtuel unique (VIP), configurez votre interface réseau CX PCA pour l'équilibrage de charge transparent. Pour plus d'informations, voir «Configuration de l'interface CX PCA avec équilibrage de charge transparent».

Si votre déploiement de serveur Web n'utilise pas d'équilibreur de charge et qu'il ne fonctionne pas sous un IP virtuel unique (VIP), vous pouvez configurer votre interface réseau CX PCA sans équilibrage de charge transparent. Pour plus d'informations, voir «Configuration de l'interface CX PCA sans équilibrage de charge transparent», à la page 49.

Configuration de l'interface CX PCA avec équilibrage de charge transparent

Vous pouvez configurer l'interface réseau de votre Application de capture passive CX avec l'équilibrage de charge transparent. Pour plus d'informations sur les avantages de l'activation de l'équilibrage de charge transparent, voir «Présentation de l'équilibrage de charge transparent de d'CX PCA», à la page 8.

Pour configurer l'interface PCA avec l'équilibrage de charge transparent, procédez comme suit :

1. Ouvrez la console Web de la CX PCA. Voir «Configuration à l'aide de la console Web», à la page 41.
2. Cliquez sur l'onglet **Interface**.
3. Sélectionnez l'option **Activer l'équilibrage de charge transparent**.
4. Entrez le nombre d'instances `Reassd` que vous souhaitez exécuter. Le fait d'augmenter le nombre d'instances `Reassd` augmente le nombre d'instances PCA pouvant traiter des paquets TCP.

   Remarque : Vous pouvez activer jusqu'à *N*-1 paquets, où *N* représente le nombre total de coeurs de processeur sur votre serveur. Par exemple, si votre serveur est équipé d'un total de 8 coeurs de processeur, vous pouvez exécuter jusqu'à 7 instances.
5. Pour vider les informations de session SSL de `memcache` lors du redémarrage du service CX PCA, sélectionnez **Redémarrer le serveur Memcached au redémarrage de Capture**.
6. Pour désactiver le total de contrôle des paquets TCP, sélectionnez Désactiver la validation du total de contrôle des paquets.

Remarque : Si le total de contrôle des paquets est activé dans votre carte d'interface réseau, il est recommandé de désactiver le total de contrôle des paquets.

7. L'option **Capture de plusieurs instances** ne doit pas être sélectionnée, sauf si vous voulez retourner à un mode sans équilibrage de charge transparent.
8. Pour entrer une règle de filtrage, recherchez l'option **Règles de filtrage**, entrez les informations relatives à votre filtre, puis cliquez sur **Créer filtre**.
9. Cliquez sur **Enregistrer les modifications** pour enregistrer les modifications que vous avez apportées à la configuration de la CX PCA. Pour annuler vos modifications, cliquez sur **Annuler les modifications**.

Configuration de l'interface CX PCA sans équilibrage de charge transparent

Pour configurer l'interface CX PCA dans un environnement sans équilibrage de charge :

1. Ouvrez la console Web de la CX PCA. Voir «Configuration à l'aide de la console Web», à la page 41.
2. Cliquez sur l'onglet **Interface**.
3. Si l'option **Activer l'équilibrage de charge transparent** est sélectionnée, désélectionnez-la. Pour plus d'informations sur les avantages de l'activation de l'équilibrage de charge transparent, voir «Présentation de l'équilibrage de charge transparent de d'CX PCA», à la page 8.
4. Ajoutez une instance CX PCA en cliquant sur **Ajouter une instance**. Vous pouvez ajouter des instances de CX PCA supplémentaires pour capturer le trafic réseau. Chaque instance de CX PCA nécessite l'utilisation d'un coeur de processeur supplémentaire. Vous pouvez ajouter jusqu'à *N*-1 instances, où *N* représente le nombre total de coeurs de processeur dans votre serveur CX PCA. Par exemple, si votre système est équipé de huit coeurs de processeur, vous pouvez activer sept instances de CX PCA.
5. Vous pouvez utiliser des numéros de port par défaut pour définir les numéros de port dans les règles de filtrage en cliquant sur **Renseigner les ports**. Les numéros de port par défaut sont compris entre 1024 et 65535. Pour filtrer des numéros de port différents pour une instance de CX PCA, vous pouvez ajouter une règle de filtrage ou modifier l'instance.
6. Pour modifier les paramètres d'une instance, recherchez Liste des instances et cliquez sur **Modifier** en regard de l'instance, afin de commencer à apporter vos modifications. Vous pouvez également supprimer une instance en cliquant sur **Supprimer** ou supprimer les règles de filtrage d'une instance en cliquant sur **Effacer les filtres**.
   a. Si vous installez CX PCA pour la première fois, éditez les filtres de chaque instance CX PCA. Voir «Modification des filtres», à la page 86.
   b. A partir du menu déroulant de l'interface principale, sélectionnez le périphérique réseau à écouter.
      - Dans la plupart des cas, vous ne devez pas écouter un périphérique dont l'adresse IP est affichée dans le menu déroulant.
      - Si le message d'état `down` est affiché pour un périphérique, le système d'exploitation n'est pas configuré pour l'activer, mais cela reste exceptionnel.
      - Pour une configuration simple, vous pouvez conserver les valeurs par défaut des autres options de configuration.
      - Pour plus d'informations sur la définition des instances de la PCA, voir «Console Web de la PCA - Onglet Interface», à la page 71.

c. Cliquez sur **Mettre à jour** pour enregistrer vos modifications.

7. Cliquez sur **Enregistrer les modifications** pour appliquer vos modifications à la CX PCA. Pour annuler vos modifications, cliquez sur **Annuler les modifications**.

La CX PCA est désormais configurée pour capturer le trafic de la carte d'interface réseau sélectionnée.

Configuration de la distribution des hits

La section suivante contient des informations sur la configuration de la distribution des hits.

Distribution de hits au serveur de traitement

Vous pouvez à présent définir le serveur de traitement ou le serveur HBR devant recevoir les données des hits envoyées par la PCA.

- Le numéro du port de destination du serveur de traitement destinataire est défini pour chaque pipeline de Windows. Voir section "TMS Pipeline Editor" du *Manuel d'administration d'IBM Tealeaf cxImpact*.

1. Cliquez sur «Console Web de la PCA - Onglet Distribution», à la page 92.
2. Cliquez sur **Ajouter**.
3. Saisissez le nom d'hôte ou l'adresse IP du serveur de traitement.
   - Si vous utilisez le HBR, saisissez le nom d'hôte ou l'adresse IP de la machine HBR. Voir section "Agent de session Health-Based Routing (HBR)" du *Manuel de configuration d'IBM Tealeaf CX*.
4. Saisissez le numéro de port. Par défaut cette valeur est `1966`.
5. Cliquez sur **OK**.
6. Cliquez sur **Enregistrer les modifications**.
7. Pour tester le débit de votre connexion, cliquez sur les liens **Ping** et Vitesse de l'hôte que vous venez d'ajouter dans l'onglet **Distribution**.
   - Si les tests échouent ou qu'ils indiquent un débit lent, modifiez la configuration de votre réseau et de la PCA.

Remarque : si vous disposez de plusieurs destinataires cible, assurez-vous de sélectionner le mode de distribution approprié. Voir «Console Web de la PCA - Onglet Distribution», à la page 92.

La configuration est paramétrée pour distribuer du trafic au serveur de traitement référencé.

- Voir «Console Web de la PCA - Onglet Distribution», à la page 92.

Horloge de référence de la PCA

Si nécessaire, vous pouvez configurer IBM Tealeaf Application de capture passive CX pour que son heure locale soit basée sur le service de transport Tealeaf. Lorsqu'elle est activée, la PCA interroge le service de transport à intervalles réguliers pour obtenir l'heure. Pour éviter toute différence, la PCA ajuste son horaire pour se rapprocher au plus de l'heure locale de l'horloge de référence.

Remarque : vous devez configurer la PCA pour qu'elle se synchronise en utilisant un des homologues de distribution en tant que source, à moins que vous ne synchronisiez l'heure d'une autre manière. Suivez les étapes ci-dessous pour la configuration.

1. Cliquez sur «Console Web de la PCA - Onglet Distribution», à la page 92.

2. Dans le panneau Utiliser le service de transport Tealeaf comme horloge de référence, saisissez le nom de l'hôte ou de l'adresse ainsi que le numéro de port du service de transport Tealeaf utilisé comme source principale pour définir l'heure.
   - Ces valeurs doivent être définies selon un des homologues de distribution configurés au préalable.
   - S'il n'est pas spécifié, le numéro de port par défaut est 1966.
- Voir «Console Web de la PCA - Onglet Distribution», à la page 92.

Distribution de hits de statistiques

Si vous le souhaitez, vous pouvez configurer la PCA afin de transmettre des informations statistiques au serveur de traitement, qui seront intégrées dans la base de données TL_STATISTICS afin de générer des rapports par le biais du portail.

- Parallèlement aux statistiques du canister et de l'agent de session du découpleur étendu, les hits de statistiques de la PCA sont disponibles sur la page Statistiques système. Voir section "Statistiques système" du *Manuel d'administration d'IBM Tealeaf cxImpact*.

1. Cliquez sur «Console Web de la PCA - Onglet Distribution», à la page 92.
2. Dans la zone Transmettre les statistiques au service de transport Tealeaf, configurez les options suivantes :
   a. Pour activer la distribution, cochez la case **Activé**.
   b. Saisissez le nom d'hôte ou l'adresse de l'homologue de distribution devant recevoir les hits de statistiques.

      Remarque : en règle générale, les hits de statistiques sont envoyés à l'homologue de distribution qui reçoit les hits capturés, tel qu'il a été défini.
   c. Indiquez un intervalle (en secondes) pour l'envoi des hits.
   d. Saisissez le numéro de port que doit écouter l'homologue de distribution. Par défaut, cette valeur est 1966.
   e. Pour utiliser le transfert sécurisé, cochez la case **Utiliser SSL**.
- Voir «Console Web de la PCA - Onglet Distribution», à la page 92.

Configuration du pipeline de la PCA

Cette section présente les options de configuration de base du pipeline de traitement d'IBM Tealeaf Application de capture passive CX.

- La configuration du pipeline de la PCA s'effectue à partir de l'onglet Pipeline de la console Web de la PCA. Voir «Console Web de la PCA - Onglet Pipeline», à la page 101.

  Remarque : le pipeline de la PCA possède une configuration différente de celle du pipeline de Windows basée sur un agent de session. Pour plus d'informations sur la configuration du pipeline de Windows, voir section "Configuration initiale du pipeline" du *Manuel de configuration d'IBM Tealeaf CX*.

Mise en sessions des données

Si les cookies sont insérés dans la demande uniquement pour identifier les visiteurs, il est possible de configurer la PCA pour effectuer la mise en sessions à partir de ces cookies. Tealeaf prend en charge plusieurs mécanismes permettant de créer des sessions Tealeaf.

- La méthode conseillée pour créer des sessions est d'utiliser Tealeaf Cookie Injector, une méthode simple côté serveur permettant d'injecter des

identificateurs uniques en tant que cookies dans les données de demande. Voir section "Installation et configuration de Tealeaf Cookie Injector" du *Manuel d'IBM Tealeaf Cookie Injector*.
- Pour une présentation générale des méthodes de mise en sessions prises en charge, voir section "Gestion de la mise en sessions des données dans Tealeaf CX" du *Manuel d'installation d'IBM Tealeaf CX*.
- Voir «Console Web de la PCA - Onglet Pipeline», à la page 101.

Mode de capture

Vous pouvez configurer IBM Tealeaf Application de capture passive CX pour capturer les types de données de demande et de réponse texte recommandés (mode Business), ou configurer les données et les fichiers binaires du mode Business, par exemple des images (mode BusinessIT).
- Le mode BusinessIT requiert plus de mémoire système.
- Voir «Console Web de la PCA - Onglet Pipeline», à la page 101.

Méthodes de demande de capture

Vous pouvez indiquer l'une des combinaisons suivantes pour les méthodes de demande :
- `GET`
- `POST`
- `PUT`
- Voir «Console Web de la PCA - Onglet Pipeline», à la page 101.

Niveau de temps

Il est possible d'attribuer des niveaux aux dates et heures identifiées par la PCA en fonction de l'interpolation entre les horodatages des paquets réseau. Vous pouvez attribuer des valeurs de seuil et des niveaux à la génération des pages par le serveur Web, l'attente dans le réseau et les durées de la boucle.
- Pour plus d'informations générales sur les niveaux de temps, voir Chapitre 6, «Mesure des performances», à la page 215.
- Pour plus d'informations sur la notification des niveaux de temps, voir section "Analyse des performances" du *Guide de notification d'IBM Tealeaf*.
- Pour plus d'informations sur la configuration des niveaux de temps, voir «Console Web de la PCA - Onglet Pipeline», à la page 101.

Traitement des hits

Consultez toutes les options disponibles concernant le traitement des hits par la PCA avant de les transférer à l'homologue de distribution. Ces paramètres peuvent affecter la configuration du stockage et les performances de la PCA.
- Voir «Console Web de la PCA - Onglet Pipeline», à la page 101.

Autres inclusions et exclusions de capture

Vous pouvez également configurer la PCA afin de capturer ou de supprimer de la capture certains types de fichiers, types Mime et tous les types de POST.
- Voir «Console Web de la PCA - Onglet Pipeline», à la page 101.

Configuration de la confidentialité

Remarque : avant d'activer la capture, vous devez configurer les règles de confidentialité afin d'éviter toute capture involontaire d'informations sensibles, par exemple le numéro de carte de crédit des clients. Si la capture est activée alors qu'aucune règle de confidentialité appropriée n'est définie, les données des clients

non filtrées peuvent être envoyées vers le pipeline de Windows et stockées dans les bases de données de Tealeaf, qui peuvent être consultées par tous les utilisateurs Tealeaf bénéficiant des droits nécessaires.

La confidentialité Tealeaf permet de manipuler, de masquer ou de supprimer des informations sensibles dans le trafic des demandes ou des réponses. En fonction des règles de confidentialité que vous avez définies, il est possible de masquer ces données dans le trafic stocké dans les bases de données de Tealeaf.

1. Premiers pas concernant la confidentialité de Tealeaf : voir chapitre "Gestion de la confidentialité des données dans Tealeaf CX" du *Manuel d'installation d'IBM Tealeaf CX*.
2. Confidentialité dans la PCA : vous pouvez déployer des règles de confidentialité à partir de la console Web de la PCA. Voir «Téléchargement de la configuration de confidentialité», à la page 118.

Activation de la capture

Remarque : les étapes suivantes permettent à la PCA de capturer le trafic réseau passant par la carte d'interface réseau spécifiée et de transférer les données capturées vers le serveur de traitement sélectionné. Lorsque le serveur de traitement n'est pas encore configuré pour capturer et traiter les données transférées, celles-ci seront perdues si la PCA ne parvient pas à établir une connexion. Cependant, vous pouvez utiliser ces étapes et celles qui suivent pour vérifier les opérations de la PCA.

Lorsque la capture est activée, le serveur de traitement doit également capturer pour que les hits soient capturés.

1. Cliquez sur «Console Web de la PCA - Onglet Console», à la page 70.
2. Cliquez sur **Démarrer**.

La PCA commence à capturer et à transférer les données vers le serveur de traitement spécifié.

- Voir «Console Web de la PCA - Onglet Console», à la page 70.

Test de votre configuration

Après avoir terminé la configuration initiale, vous pouvez effectuer les étapes suivantes afin de la vérifier.

Il est difficile de consulter la sortie d'IBM Tealeaf Application de capture passive CX avant que le reste du système IBM Tealeaf CX ne soit configuré. Si vous configurez uniquement la PCA, vous pouvez suivre les étapes ci-dessous afin de vous assurer que le programme fonctionne correctement.

1. Activez la capture à partir de la console Web de la PCA, si elle ne l'est pas déjà. Vérifiez que la capture est activée. Voir «Activation de la capture».
2. Lorsque la capture fonctionne, consultez la section Santé de la machine dans l'onglet Récapitulatif afin de vous assurer que tous les processus sont en cours d'exécution.
   - Dans la section Homologues, les homologues de distribution doivent être répertoriés. La colonne Etat doit indiquer `connected`. Des erreurs peuvent s'afficher ici lorsqu'un serveur de traitement Tealeaf n'est pas configuré pour recevoir des données de la PCA.

- Dans la section Homologues, les statistiques `Hits Delivered` doivent être différentes de zéro et en augmentation, indiquant que la PCA distribue les hits aux cibles définies dans l'onglet Distribution.
- Voir «Console Web de la PCA - Onglet Récapitulatif», à la page 60.

3. Consultez les fichiers journaux pour prendre connaissance des erreurs. Voir «Console Web de la PCA - Onglet Journaux de sauvegarde», à la page 159.
   - Les fichiers journaux contiennent des erreurs indiquant que la PCA n'est pas en mesure de contacter un homologue lorsqu'un serveur de traitement Tealeaf n'est pas configuré pour recevoir des données de la PCA.

Lorsque tous les composants Tealeaf sont configurés, vous devez effectuer un test de bout en bout.

Navigateurs pris en charge pour la console Web de la PCA

Les navigateurs suivants sont pris en charge pour accéder à la console Web de la PCA :

- Microsoft Internet Explorer 7, 8, et 9
- Firefox 4 ou version supérieure

Remarque : les navigateurs pris en charge pour accéder à la console Web de la PCA sont différents de ceux utilisés pour accéder au Portail Tealeaf. L'utilisation d'un navigateur non pris en charge peut générer des comportements inattendus.

- Voir section "Connexion au Portail Tealeaf" du *Manuel de l'utilisateur d'IBM Tealeaf cxImpact*.

Connexion à la console Web de la PCA

Vous pouvez utiliser la console Web, outil d'administration basé sur le Web, pour contrôler et configurer le serveur IBM Tealeaf Application de capture passive CX.

Pour ouvrir la console Web, saisissez l'adresse suivante dans la zone **Adresse** de votre navigateur.
Par HTTP sécurisé :

```
https://<servername>:<portnumber>
```

Par HTTP

```
http://<servername>:<portnumber>
```

où :

- `<servername>` correspond au nom d'hôte du serveur de la PCA.
- `<portnumber>` correspond au numéro de port utilisé pour communiquer avec la console Web.
  - Pour la connexion HTTP, le numéro de port par défaut est `8080`.
  - Pour la connexion HTTPS, le numéro de port par défaut est `8443`.

Il est possible de configurer les ports que la console Web de la PCA écoute. Voir «Modification des ports d'écoute de la console Web», à la page 57.

Remarque : si vous activez les options de Windows Enhanced Security, il se peut que vous rencontriez certains problèmes lorsque vous tentez d'accéder à la console Web de la PCA par le biais d'Internet Explorer. Voir section "Traitement des incidents - Portail" du *Guide de dépannage d'IBM Tealeaf*.

Déconnexion de la console Web de la PCA

Fermez la fenêtre du navigateur pour vous déconnecter de la PCA.

Remarque : à partir de PCA Build 3500, la console Web impose un délai d'attente de 30 minutes. Si la PCA interrompt votre session, vous devez vous connecter, que l'authentification soit activée ou non.

- Si votre session a expiré, saisissez à nouveau vos données d'identification pour vous reconnecter.
- Si l'authentification est désactivée, ne renseignez pas les zones de texte et cliquez sur **Connexion**.
- Pour plus d'informations sur la configuration du délai d'attente, voir «Console Web de la PCA - Onglet Console», à la page 70.

Onglets de la console Web

Vous trouverez les informations d'état en haut de la console Web. Elles comprennent le numéro de build de Tealeaf, les informations sur l'hôte et le port, la version actuelle de Linux ainsi que l'heure du dernier chargement de la page.

- Dans le coin supérieur droit de la console, vous pouvez accéder à la page InfoSys. Voir «Page InfoSys», à la page 58.
- Lorsque la page est chargée, la console Web vérifie l'espace disque disponible sur la partition contenant le logiciel de la PCA. Si l'espace libre est insuffisant, un message d'état s'affiche en rouge et vous devez suivre les étapes afin de libérer immédiatement de l'espace sur la partition (`/usr/local/ctccap` par défaut).

Les pages de configuration suivantes sont disponibles dans la console Web :

Libellé de l'onglet
: Utilisé pour...

«Console Web de la PCA - Onglet Récapitulatif», à la page 60
: Statuts d'exécution des processus de capture ; affichage des hits, hits rejetés ; connexions/paquets/erreurs TCP ; connexions/établissements de liaison SSL ; programme d'écoute des octets lus et écrits Affichage des statuts et des informations de configuration des interfaces réseau principale et secondaire

«Console Web de la PCA - Onglet Console», à la page 70
: Démarrage/arrêt de la capture des paquets opérationnels du réseau, activation/désactivation de la capture au démarrage

«Console Web de la PCA - Onglet Interface», à la page 71
: Définition des interfaces réseau (cartes d'interface réseau), configuration de Passive Capture pour un tap réseau ou un port de commutation mis en miroir, configuration des instances de capture, définition des serveurs Web à gérer et à ignorer, définition des filtres du trafic et définition des paramètres d'optimisation pour la capture

«Console Web de la PCA - Onglet Distribution», à la page 92
: Définition des serveurs Tealeaf pour la réception des paquets de hits envoyés par Passive Capture, paramétrage de la distribution, synchronisation de l'heure

«Console Web de la PCA - Onglet Clés SSL», à la page 97
Chargement, modification et suppression de clés privées pour les serveurs Web surveillés ; informations supplémentaires pour ignorer ou supprimer les clés privées manquantes

«Console Web de la PCA - Onglet Pipeline», à la page 101
Modification des paramètres de configuration contrôlant le traitement des hits ; niveaux de temps, mode de capture, mise en sessions, extensions incluses/exclues

«Téléchargement de la configuration de confidentialité», à la page 118
Activation/désactivation des paramètres de confidentialité, création et modification des règles de confidentialité

«Statistiques par instance», à la page 137
Affichage des indicateurs de l'activité de Passive Capture

«Console Web de la PCA - Onglet Journaux de sauvegarde», à la page 159
Sauvegarde et chargement du fichier de configuration ; affichage des fichiers journaux ; activation/désactivation de l'archivage des paquets

«Console Web de la PCA - Onglet Reprise», à la page 161
Gestion des paramètres de la reprise

«Console Web de la PCA - Onglet Utilitaires», à la page 163
Accès à de nombreux utilitaires pour les administrateurs de la PCA

«Console Web de la PCA - Page Débogage», à la page 168
Gestion des images-mémoire de la PCA

Configuration

Les sections suivantes contiennent quelques étapes de base pour configurer la console Web de la PCA.

Activation de l'authentification pour la console Web

Il est possible de restreindre l'accès à la console Web de la PCA. Voir Chapitre 9, «Configuration matérielle et installation du système d'exploitation», à la page 235.

Changement d'accès HTTP/HTTPS

Par défaut, il est possible d'accéder à la console Web de la PCA en mode HTTP via le port 8080 ou HTTPS via le port 8443.

Si vous le souhaitez, vous pouvez configurer la PCA pour ne pouvoir y accéder que par un seul de ces modes.

Etapes :
Pour changer le mode d'accès, suivez les étapes ci-dessous.

1. Modifiez le fichier `/usr/local/ctccap/etc/runtime.conf`.
2. Ajoutez ou modifiez les lignes suivantes :

```
httpd_port_enable="NO"
httpd_portssl_enable="YES"
```

Mode **Options**

HTTP uniquement

```
httpd_port_enable="YES"
httpd_portssl_enable="NO"
```

HTTPS uniquement

```
httpd_port_enable="NO"
httpd_portssl_enable="YES"
```

HTTP et HTTPS

```
httpd_port_enable="YES"
httpd_portssl_enable="YES"
```

3. Enregistrez le fichier.
4. Redémarrez la PCA.

Si nécessaire, vous pouvez modifier les ports écoutés par la console Web de la PCA. Voir «Modification des ports d'écoute de la console Web».
Pour plus d'informations sur la connexion à la console Web, voir «Connexion à la console Web de la PCA», à la page 54.

Déploiement d'un certificat SSL pour la console Web

Vous pouvez déployer un certificat SSL personnalisé. Voir «Création d'un certificat autosigné», à la page 207.

Modification des ports d'écoute de la console Web

Par défaut, la console Web de la PCA écoute les ports répertoriés au début de cette section. Si vous le souhaitez, vous pouvez modifier les ports d'écoute en ajoutant les lignes suivantes dans le fichier `runtime.conf`.

Le fichier `runtime.conf` est un substitut aux paramètres par défaut stockés dans le fichier `tealeaf.conf`.

Remarque : `tealeaf.conf` doit être configuré en lecture seule et ne doit jamais être modifié.

1. Modifiez `runtime.conf`, situé à l'emplacement suivant :
   `/usr/local/ctccap/etc/runtime.conf`
2. Port HTTP (non chiffré) : ajoutez les lignes suivantes :
   ```
   httpd_listen="X"
   httpd_port="X"
   ```
   où `X` correspond au numéro de port que la console Web doit écouter pour le trafic non chiffré.
3. Port HTTPS (chiffré) : ajoutez les lignes suivantes :
   ```
   httpd_listenssl="X"
   httpd_portssl="X"
   ```
   où `X` correspond au numéro de port que la console Web doit écouter pour le trafic chiffré.
4. Enregistrez le fichier.
5. Redémarrez la PCA.

Prise en charge du format IPv6 dans la console Web de la PCA

Pour les nouvelles installations de PCA Build 3600, la console Web est configurée pour accepter les adresses IP au format IPv6 par défaut.

- Pour les versions antérieures à PCA Build 3502, il n'est pas possible de saisir les adresses au format IPv6 via la console Web de la PCA.

Si vous effectuez une mise à niveau à partir d'une version antérieure, vous devez insérer manuellement l'attribut suivant dans la section `Conf` du fichier `ctc-conf.xml` :

```
<IPv6ConsoleEnabled>1</IPv6ConsoleEnabled>
```

Cette modification peut également s'appliquer à PCA Build 3502 pour configurer la console Web de la PCA afin d'accepter par défaut les adresses au format IPv6.

- Voir «Fichier de configuration Passive Capture `ctc-conf.xml`», à la page 171.

Lorsque la valeur est définie à 1, la console Web de la PCA valide l'entrée de données en supposant que les adresses IP sont saisies au format IPv6.

- Cette modification concerne essentiellement les adresses que vous pouvez saisir dans l'onglet Interface. Voir «Console Web de la PCA - Onglet Interface», à la page 71.

Page InfoSys

Lorsque vous cliquez sur le lien infosys au-dessus de la barre de menus **Console de la PCA**, la page InfoSys s'affiche. Cette page est générée lorsqu'un ensemble de commandes Linux est exécuté par le biais de la ligne de commande et que les résultats s'affichent dans une page unique.

Vous pouvez consulter les commandes individuelles permettant de générer la page InfoSys et les exemples de sorties de chaque commande.

Système

Vous pouvez utiliser la commande suivante pour les distributions SLES et RHEL possédant des noms de fichier différents.

Commande

```
cat /etc/*-release
```

Sortie

```
Système
informations sur l'édition                 : LSB_VERSION="1.3"
Red Hat Enterprise Linux ES édition 3 (Taroon mise à jour 5)
```

Commande

```
uname-a
```

Sortie

```
informations sur le noyau
: Linux venus.tealeaf.com 2.4.21-32.EL #1 Fri \
> 15 avril 21:29:19 EDT 2005 i686 i686 i386 GNU/Linux
```

Commande

```
cat /proc/cpuinfo
```

Sortie

```
processor                     : 0
vendor_id                    : GenuineIntel
cpu family                    : 6
model                            : 8
model name               : Pentium III (Coppermine)
stepping   : 3
cpu MHz                       : 664.526
cache size                    : 256 KB
```

```
fdiv_bug  : no
hlt_bug                         : no
f00f_bug  : no
coma_bug                   : no
fpu                                  : yes
fpu_exception           : yes
cpuid level                   : 2
wp                                  : yes
flags                               : fpu vme de pse tsc msr pae mce cx8 sep \
> mtrr pge mca cmov pat pse36 mmx fxsr sse
bogomips                     : 1327.10
```

Commande

```
cat /proc/meminfo
```

Sortie

```
total:    used:    free:  shared: buffers:  cached:
Mem:  258945024 250028032  8916992        0 110923776 90759168
Swap: 534601728  5242880 529358848
MemTotal:       252876 kB
MemFree:          8708 kB
MemShared:           0 kB
Buffers:        108324 kB
Cached:          85572 kB
SwapCached:       3060 kB
Active:         183328 kB
ActiveAnon:      37496 kB
ActiveCache:    145832 kB
Inact_dirty:     35704 kB
Inact_laundry:    7588 kB
Inact_clean:      3436 kB
Inact_target:    46008 kB
HighTotal:           0 kB
HighFree:            0 kB
LowTotal:       252876 kB
LowFree:          8708 kB
SwapTotal:      522072 kB
SwapFree:       516952 kB
CommitLimit:    648508 kB
Committed_AS:   285972 kB
HugePages_Total:     0
HugePages_Free:      0
Hugepagesize:     4096 kB
```

dmesg

Commande

```
dmesg
```

Sortie

```
dmesg
device eth2 entered promiscuous mode
device eth0 left promiscuous mode
device eth4 left promiscuous mode
device eth1 left promiscuous mode
device eth2 left promiscuous mode
device eth0 entered promiscuous mode
eth4: Promiscuous mode enabled.
device eth4 entered promiscuous mode
device eth1 entered promiscuous mode
eth2: Setting promiscuous mode.
device eth2 entered promiscuous mode
```

Console Web de la PCA - Onglet Récapitulatif

Lorsque vous vous connectez à la console Web, l'onglet **Récapitulatif** s'affiche. Il donne un aperçu de l'état du système. Les statistiques affichées sur cette page concernent l'intégrité, les connexions, les statistiques TCP et SSL en cours, les connexions HTTP et les mesures de la partition.

- Des statistiques des composés sont aussi fournies pour une meilleure compréhension de la présentation de l'intégrité de la PCA. Voir «Statistiques des composés de l'instance».
- Si la PCA génère une image-mémoire, vous trouverez un lien vers la page Débogage dans l'onglet **Récapitulatif**. Voir «Console Web de la PCA - Page Débogage», à la page 168.
- Vous trouverez des informations supplémentaires sur le système d'exploitation dans l'onglet Utilitaires. Voir «Console Web de la PCA - Onglet Utilitaires», à la page 163.

Statistiques des composés de l'instance

Instance Compound Statistics

ID	Status	Descripton
0	70.26 %	The percentage of alien packets
1	false	If true, reassd cannot keep up with listend.
1	0 %	The percentage of dropped packet connections
0	1 %	The percentage becoming unidirectional traffic
0	96 hits/sec	The rate reassd is currently reassembling non-SSL hits.
1	false	If true, encountered Diffie Hellman SSL
0	0.65 %	The percentage of aged connections
0	3 keys/sec	Missing SSL keys/sec
0	2730 kbytes/sec	Filtered traffic kbytes/sec
1	0 hits	If non-zero, hits are being dropped due to an overloaded pipelined.
1	0 packets	If non-zero, packets are being dropped because they exceed the max size limit.

Figure 3. Onglet Récapitulatif - Statistiques des composés de l'instance

Par défaut, la page Récapitulatif s'actualise automatiquement environ toutes les 20 secondes.

- Pour désactiver la fonction d'actualisation automatique, cliquez sur **Désactiver l'actualisation automatique** en haut à droite de la page. La page ne s'actualise plus automatiquement jusqu'à ce qu'un utilisateur quitte la page et y revienne ou que la fonction soit à nouveau activée. .
- Pour actualiser manuellement les données, cliquez sur **Actualiser**.

Lorsque la PCA rencontre des problèmes lors de la capture ou du traitement des données de hit, un message contenant des informations relatives au problème peut s'afficher dans l'onglet **Récapitulatif**.

- Les éléments répertoriés en rouge doivent être considérés en priorité.
- Pour plus d'informations sur l'évaluation de ces messages, voir «Informations de débogage supplémentaires de la console Web de la PCA», à la page 69.

Le pourcentage de paquets étrangers

Il s'agit du pourcentage de paquets contenus dans le flux de capture que la PCA n'est pas en mesure d'associer à une connexion existante. Lors de la première capture, il est possible que ce pourcentage soit élevé, mais il doit diminuer dans la mesure où la capture continue d'associer et de traiter les hits.

Analyse :
Si cette valeur est inscrite en rouge, il est nécessaire d'améliorer la qualité des données envoyées vers la PCA ou des connexions TCP. Vous trouverez ci-dessous quelques conseils.

1. Appliquer des filtres pour le trafic : si vous ne l'avez pas encore fait, vous pouvez appliquer des filtres pour supprimer le trafic indésirable transféré vers la PCA. Il est possible d'appliquer des filtres sur des plages de ports ou des adresses IP.
   - Voir «Console Web de la PCA - Onglet Interface», à la page 71.
2. Mode de capture : si la PCA est configurée en mode BusinessIT, il est possible qu'un plus grand nombre de données inutiles soient capturées. Le nombre de paquets étrangers peut diminuer si vous passez en mode Business. Voir «Console Web de la PCA - Onglet Pipeline», à la page 101.
3. Après avoir effectué les modifications ci-dessus, redémarrez la PCA. Voir Chapitre 2, «Installation», à la page 17.
4. Vérifier le matériel : il est possible que le miroir de port utilisé pour distribuer les hits en supprime quelques-uns lorsqu'il est surchargé. Contactez votre service informatique pour vous assurer que le miroir de port ne perd pas de données.
   - Si le nombre de paquets étrangers et de pages manquantes est élevé, la carte d'interface réseau de la machine qui héberge la PCA ne fonctionne peut-être pas correctement. Vous devez également, si nécessaire, modifier et mettre à jour le pilote de la carte d'interface réseau.
5. Totaux de contrôle incorrects : s'ils sont nombreux, contactez votre service informatique pour vérifier que la source du trafic transféré vers la PCA génère des totaux de contrôle valides.
   - Pour tester la validité des totaux de contrôle dans les paquets de données, vous pouvez activer la validation de total de contrôle à partir de l'onglet Interface. Elle est activée par défaut. Voir «Console Web de la PCA - Onglet Interface», à la page 71.
6. Vous trouverez des informations supplémentaires dans le journal des statistiques disponible à partir de la console Web de la PCA. Voir «Console Web de la PCA - Onglet Journaux de sauvegarde», à la page 159.
7. Dans la PCA, vous pouvez activer l'archivage permettant de distribuer des paquets réseau bruts vers des archives spécifiées et de déboguer les problèmes des données de session.

   Remarque : l'archivage de la PCA doit être utilisé sous le contrôle du personnel Tealeaf. Pour plus d'informations, contactez Tealeaf Customer Support .
   - Voir «Console Web de la PCA - Onglet Journaux de sauvegarde», à la page 159.

Si true, reassd ne peut pas suivre listend

Le processus d'écoute (listend) de l'instance de la PCA envoie plus de hits vers le processus de réassemblage (reassd) qu'il ne peut en évaluer. Par conséquent, les hits sont supprimés.

- Pour plus d'informations sur le traitement des flux dans la PCA, voir Chapitre 1, «Présentation de Passive Capture», à la page 1.

Analyse :
Si cette valeur est inscrite en rouge, vous devez configurer la PCA pour envoyer moins de hits par le biais de l'instance individuelle de la PCA. Quelques conseils :

1. Ajouter des instances de la PCA : le fait d'ajouter des instances d' IBM Tealeaf Application de capture passive CX au serveur hôte peut permettre d'alléger le volume du trafic de chaque processus.
   - Pour plus d'informations sur le nombre maximal d'instances sur le serveur, voir Chapitre 2, «Installation», à la page 17.
   - Pour plus d'informations sur l'ajout d'instances, voir «Console Web de la PCA - Onglet Interface», à la page 71.
2. Ajouter des ports d'écoute : le fait d'ajouter des ports d'écoute à la PCA peut permettre de réduire les goulots d'étranglement lors du traitement sur chaque port. Voir «Console Web de la PCA - Onglet Interface», à la page 71.

Pourcentage de connexions dont les paquets ont été abandonnés

Cette mesure identifie les connexions établies pour lesquelles la PCA suspecte un abandon des paquets.

Analyse :
La connexion entre la PCA et l'unité qui l'alimente est à l'origine du problème. Modifiez la configuration d'écoute de la PCA, la configuration de sortie de l'unité d'envoi et la topologie de réseau faisant la liaison.

- Pour plus d'informations sur la configuration des interfaces réseau écoutées par la PCA, voir «Console Web de la PCA - Onglet Utilitaires», à la page 163.

Pourcentage de trafic unidirectionnel

Cette valeur indique le pourcentage de trafic transféré vers la PCA et circulant dans une seule direction. Pour réassembler un hit, la PCA met en corrélation des demandes (trafic circulant entre un navigateur client et un serveur Web) et des réponses (messages renvoyés au navigateur client en fonction des demandes. Pour capturer l'expérience d'un visiteur, la PCA doit recevoir tout le trafic bidirectionnel.

Analyse :
Généralement, il s'agit d'un problème de configuration de l'unité chargée de transférer les données vers la PCA. Contactez votre service informatique pour vérifier que le miroir de port ou le commutateur envoie le trafic bidirectionnel sur tous les ports de Tealeaf.

- Lorsque la PCA détecte des hits unidirectionnels, il est probable qu'ils soient abandonnés. Concernant les hits de type demande, ils peuvent être annulés lorsque le flux de capture ne contient aucune réponse correspondante.

Le débit reassd rassemble actuellement des hits non-SSL

Cette valeur indique la vitesse de traitement des coeurs de la PCA. En général, une instance de la PCA doit être en mesure de traiter entre 400 et 600 hits par seconde.

- Pour le trafic SSL, le débit de traitement est généralement compris entre 200 et 300 hits par seconde.

Analyse :
Si ce débit diminue trop, le processus reassd est surchargé. Prenez en compte les éléments suivants afin d'améliorer les débits de traitement :

Vérifier les règles de confidentialité : les règles appliquées dans la PCA peuvent augmenter la charge de traitement, tout particulièrement si vous utilisez des expressions régulières pour évaluer les données. Dans la mesure du possible, évitez cela en utilisant des expressions régulières.

- Utilisez des règles de confidentialité pour verrouiller ou chiffrer uniquement les données les plus sensibles. Pour plus d'informations sur les règles de confidentialité, voir «Téléchargement de la configuration de confidentialité», à la page 118.
- Au besoin, l'évaluation de la confidentialité peut être déplacée de la PCA au pipeline de Windows. Si l'application de paramètres de confidentialité dans la PCA ne laisse jamais apparaître les données sensibles dans le système Tealeaf, il est possible de configurer le traitement des données non critiques par le biais du pipeline de Windows à l'aide de la même configuration de règles. Voir section "Agent de session de confidentialité" du *Manuel de configuration d'IBM Tealeaf CX*.
- Pour plus d'informations sur les méthodes de déploiement de la confidentialité de Tealeaf, voir section "Gestion de la confidentialité des données dans Tealeaf CX" du *Manuel d'installation d'IBM Tealeaf CX*.

Si true, protocole Diffie-Hellman pour le chiffrement SSL rencontré

Si cette valeur est inscrite en rouge, la PCA a rencontré l'algorithme de chiffrement Diffie-Hellman SSL, mais il n'est pas pris en charge par la PCA.

Analyse :
IBM Tealeaf Application de capture passive CX n'est pas en mesure de capturer le trafic en présence du protocole Diffie-Hellman. Nous vous recommandons de reconfigurer vos serveurs Web afin de ne pas utiliser ce protocole. Pour plus d'informations, consultez la documentation fournie avec votre produit de serveur Web.

Pourcentage d'anciennes connexions

Cette valeur indique le pourcentage de connexions TCP ayant dépassé le délai d'attente capturées par la PCA.

- Les anciennes connexions peuvent donner lieu à des interruptions de session anormales dans les données Tealeaf.

Analyse :
Des pourcentages élevés de connexions anciennes peuvent indiquer un problème de configuration du réseau. Cela se produit lorsque le délai d'attente de la connexion indique que la PCA est en attente de données qui ne sont pas distribuées.

- Par défaut, le délai d'attente de la PCA est de 60 minutes.
- Vous pouvez configurer le délai d'attente de la connexion de la PCA par le biais du fichier `ctc-conf.xml`. Il s'agit du paramètre `<AgedTcpConnectionsTimeout>` dans la section de capture. Voir «Fichier de configuration Passive Capture `ctc-conf.xml`», à la page 171.

Clés SSL par seconde manquantes

Cette valeur indique le nombre de clés SSL manquantes détectées dans le trafic chaque seconde.

Analyse :
Lorsque cette valeur est indiquée en rouge, les clés SSL sont mises à jour sur le serveur Web, mais la PCA n'a pas encore reçu les nouvelles clés.

- Sans les clés SSL adaptées, la PCA n'est pas en mesure de déchiffrer le trafic SSL et ces hits sont supprimés.

Vous devez obtenir les nouvelles clés SSL à partir du serveur Web. Contactez l'équipe informatique qui gère vos serveurs Web.

- Pour plus d'informations sur l'installation de clés SSL pour la PCA, voir Chapitre 5, «Clés SSL», à la page 193.
- Si votre environnement utilise un module de sécurité du matériel pour la gestion des clés, une configuration supplémentaire peut être nécessaire. Voir Annexe D, «Annexe - Intégration des clés SSL de Tealeaf avec HSM», à la page 253.

Trafic de kilooctets par seconde filtré

Cette valeur indique le volume de kilooctets par seconde du trafic capturé par la PCA après l'application des règles de filtrage configurées.

Analyse :
Si cette valeur est trop faible, il se peut qu'un problème lié aux filtres de données appliqués par la PCA existe. Modifiez les filtres que vous avez appliqués.

- Voir «Console Web de la PCA - Onglet Interface», à la page 71.

Pour évaluer la qualité de votre filtrage, vérifiez la qualité des données capturées. Une relecture vous permettra d'identifier rapidement si certains hits significatifs ont été supprimés.

- Pour plus d'informations sur l'utilisation de la relecture à partir du portail Tealeaf, voir section "CX Browser Based Replay" du *Manuel de l'utilisateur d'IBM Tealeaf cxImpact*.
- Pour plus d'informations sur l'utilisation de l'application de bureauIBM Tealeaf Visualiseur CX RealiTea, voir section "RealiTea Viewer - Affichage de la réexécution" du *Manuel de l'utilisateur d'IBM Tealeaf RealiTea Viewer*.

Abandon des hits en raison d'une surcharge du processus pipelined lorsque la valeur est différente zéro.

Lorsque cette valeur est différente de zéro, le nombre indiqué de paquets TCP est abandonné du processus pipelined en raison de conditions de surcharge.

Analyse :
Cette valeur doit être différente de zéro. Vous pouvez définir la taille maximale autorisée pour chaque paquet TCP par le biais des Paramètres d'optimisation dans l'onglet Interface.

- Voir «Console Web de la PCA - Onglet Interface», à la page 71.

Si certains hits sont abandonnés, la condition de surcharge peut survenir lorsque les règles de confidentialité sont trop nombreuses ou trop complexes.

- Voir «Téléchargement de la configuration de confidentialité», à la page 118.

Dans PCA Build 3403 ou supérieure, vous pouvez ajouter des instances du processus pipelined, une solution intéressante pour répartir la charge de traitement.

- Voir «Console Web de la PCA - Onglet Pipeline», à la page 101.

Lorsque cette statistique est calculée dans toutes les instances de la PCA, le résultat indique que la totalité des hits est perdue, car leur volume dépasse la taille définie pour le paquet TCP. Pour calculer le % du total, divisez cette valeur par la somme des statistiques de `Captured before hit processing` pour toutes les instances de la PCA, qui correspond au nombre total de hits à distribuer dans la file d'attente du pipeline.

- Voir «Statistiques par instance», à la page 137.

Il est possible d'augmenter le nombre de pipelines et la taille de queue2 à partir de l'onglet Pipeline afin de résoudre ce problème.

- Voir «Console Web de la PCA - Onglet Pipeline», à la page 101.

Abandon des paquets lorsqu'ils dépassent la taille maximale autorisée quand la valeur est différente de zéro.

Lorsqu'un paquet dont la taille dépasse la taille maximale autorisée pour la capture des paquets volumineux est reçu, cette valeur est de un.

Remarque : si vous utilisez une ou plusieurs cartes d'interface réseau de 10 Go pour la connexion fibre et que vous rencontrez des problèmes de qualité lors de la capture du trafic, il est possible que des problèmes liés à la carte d'interface à fibre et aux pilotes existent. Si la PCA n'utilise pas de cartes d'interface réseau dont les composants sont produits par Intel, Tealeaf vous recommande vivement d'en obtenir une qui possède un jeu de circuits Intel.

Sous l'onglet Interface de la vue Paramètres d'optimisation, la zone `Max large capture packet size` permet de définir la taille maximale des paquets volumineux à capturer.

- Par défaut, cette valeur est définie à `8` Ko.
- Vous pouvez, si nécessaire, augmenter cette valeur pour adapter les systèmes possédant certaines fonctions, par exemple si la fonction LRO (Large Receive Offload) est activée.

Lorsque vous augmentez la valeur de la zone `Max large capture packet size`, la valeur dans l'onglet Récapitulatif doit cesser d'augmenter.

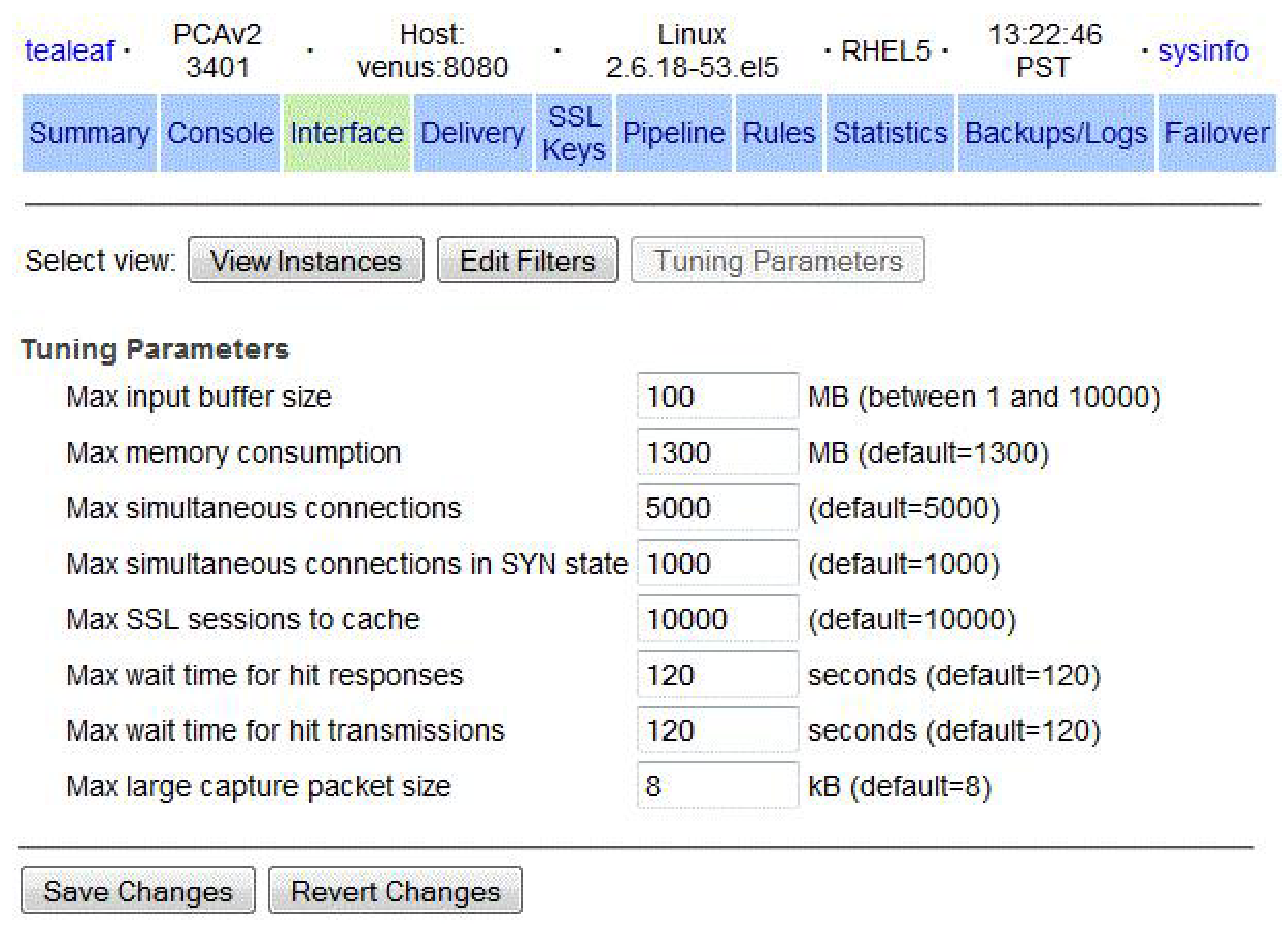


Figure 4. Taille maximale des paquets volumineux

Voir «Console Web de la PCA - Onglet Interface», à la page 71.

Connexions TCP

TCP Connections

IPv4 present	TRUE
IPv6 present	FALSE

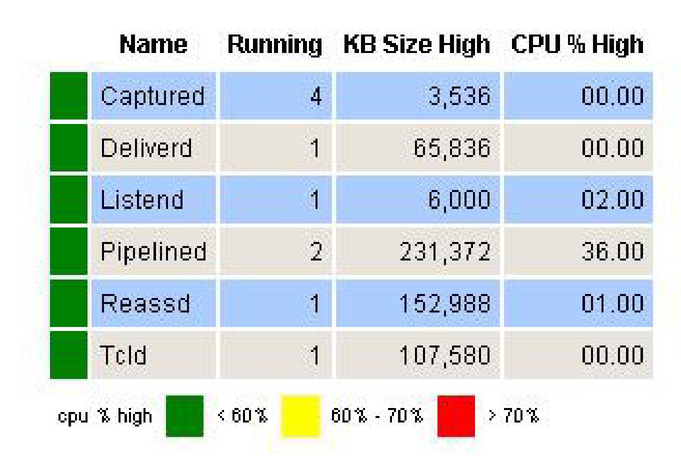
Figure 5. Onglet Récapitulatif - Connexions TCP

Remarque : le tableau Connexions TCP est affiché dans PCA Build 3500 ou supérieure où il est possible de détecter le trafic IPv6. La capture et le traitement des adresses au format IPv6 n'est pas pris en charge à partir de PCA Build 3500.

Dans le tableau Connexions TCP, vous pouvez consulter les types d'adresses IP détectés par IBM Tealeaf Application de capture passive CX. TRUE indique que le type de connexion est détecté.

Santé de la machine

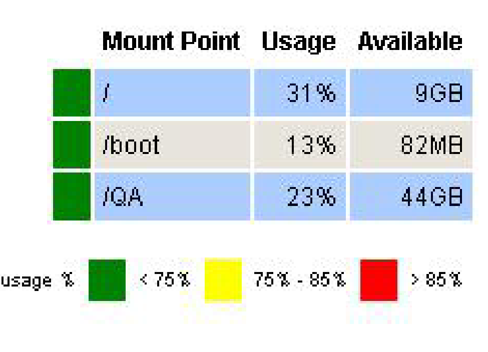
Le panneau Santé de la machine indique les mesures en cours et l'intégrité générale de chaque processus en cours d'exécution sur le serveur de la PCA.



Machine Health

Name	Running	KB Size High	CPU % High
Captured	4	3,536	00.00
Deliverd	1	65,836	00.00
Listend	1	6,000	02.00
Pipelined	2	231,372	36.00
Reassd	1	152,988	01.00
Tcld	1	107,580	00.00

cpu % high < 60% 60% - 70% > 70%



Mount Point	Usage	Available
/	31%	9GB
/boot	13%	82MB
/QA	23%	44GB

usage % < 75% 75% - 85% > 85%

Figure 6. Onglet Récapitulatif - Santé de la machine

Paramètre
Description

Nom Indique le nom du processus du pipeline de la PCA.

Processus exécutés
Indique le nombre de processus en cours d'exécution sur le serveur de la PCA.

Taille supérieure, en kilooctets
Indique le volume maximal en kilooctets utilisé par toutes les instances du processus depuis le dernier redémarrage de la PCA.

Pourcentage élevé d'UC élevé
Indique le pourcentage de consommation maximale de mémoire RAM par rapport à la mémoire disponible sur le processeur depuis le dernier redémarrage de la PCA.

Statistiques de montage

Vous pouvez consulter les statistiques des points de montage configurés sur le serveur de la PCA.

Paramètre
Description

Mount Point
Indique le chemin d'accès à partir de la racine du point de montage spécifié.

Usage Indique le pourcentage de mémoire RAM disponible utilisée par le point de montage.

Available
Indique la mémoire RAM disponible utilisée par le point de montage.

Homologues

Le panneau Homologues indique la connectivité entre le serveur de la PCA et les serveurs du service de transport qui traitent les données capturées par la PCA.

Peers

Delivery Host or Address	Port	Security	Status	Hits Delivered	Hits Dropped
127.0.0.1	1966	none	disconnected	0	0

Figure 7. Onglet Récapitulatif - Homologues

Paramètre
Description

Hôte ou adresse de livraison
Indique le nom d'hôte ou l'adresse IP statique de l'homologue.

Port
Indique le port utilisé pour communiquer avec l'homologue du service de transport.

- Le port 1966 ou 1967 est généralement utilisé.

Statut
Statut Current : disconnected ou connected

Hits livrés
Indique le nombre of hits que le processus delivered envoie à l'homologue après le dernier redémarrage de la PCA.

Hits abandonnés
Indique le nombre de hits non reconnus, et par conséquent supprimés, par l'homologue depuis le dernier redémarrage de la PCA.

Remarque : examinez de plus près les valeurs différentes de zéro avec l'aide des administrateurs du serveur du service de transport dans la mesure où elles peuvent signaler des problèmes de connectivité ou de traitement des hits au niveau du pipeline de Windows.

Statistiques Current Per Second

Pour chaque instance de la PCA, ce panneau indique le flux de hits par seconde à travers chaque processus de l'application. Par défaut, il est actualisé toutes les 20 secondes.

Current Per Second Stats

ID	Listend Packets In	Listend Out	Reassd In	TCP Connections	SSL Missing Keys	SSL New Handshakes	Reassd Hits Non-SSL	Reassd Hits SSL	Reassd Out
0	1,733	1MB	940KB	7	0	2	31	0	31

Figure 8. Onglet Récapitulatif - Statistiques Current Per Second

Paramètre
: **Description**

`Identificateur`
: Identificateur de l'instance

`Paquets entrants Listend`
: Représente le nombre de paquets entrant dans le processus listend. Cette valeur indique le débit de paquets que la PCA reçoit du réseau.

`Données sortantes Listend`
: Représente le volume de données par seconde sortant du processus listend.

`Données entrantes Reassd`
: Représente le volume de données par seconde devant entrer dans le processus reassd. Cette valeur doit correspondre au volume de données sortant du processus listend.

  - Des différences entre les valeurs de `Listend Out` et de `Reassd In` peuvent indiquer que la PCA rencontre des problèmes pour traiter rapidement les hits afin de correspondre au flux du trafic actuel.

`Connexions TCP`
: Représente le nombre de connexions TCP entre la PCA et le commutateur ou le miroir de port, en lui soumettant des données.

`Clés manquantes SSL`
: Représente le nombre de clés SSL manquantes par seconde.

  Remarque : cette valeur doit être de zéro. Dans le cas contraire, cela peut indiquer qu'il existe des problèmes. Voir «Console Web de la PCA - Onglet Clés SSL», à la page 97.

`Nouveaux établissements de liaison SSL`
: Représente le nombre d'établissements de liaison SSL détectés par seconde dans le flux de capture. Cette valeur indique le nombre de nouvelles sessions.

  Remarque : lorsque les valeurs sont constamment anormales, il est possible que le serveur Web initialise de nouveaux établissements de liaison SSL au mauvais moment, ce qui peut indiquer un problème de configuration côté serveur.

`Hits non-SSL Reassd`
: Représente le nombre de hits non-SSL entrant par seconde dans le processus reassd.

`Hits SSL Reassd`
: Représente le nombre de hits SSL entrant par seconde dans le processus reassd.

`Hits sortants Reassd`
: Représente le nombre de hits sortant par seconde du processus reassd.

Informations de débogage supplémentaires de la console Web de la PCA

- Capturez des fichiers tcpdump du trafic réseau de la PCA. Ces données peuvent permettre d'identifier si les problèmes se produisent dans la PCA ou à un autre niveau dans l'infrastructure réseau de l'entreprise.

- Vous pouvez télécharger des informations statistiques dans le journal des statistiques. Voir «Statistiques par instance», à la page 137.
- Si la PCA a généré une image-mémoire suite à une erreur critique, vous pouvez télécharger l'image-mémoire et d'autres données à partir de la page Débogage, accessible via un lien de l'onglet Récapitulatif. Voir «Console Web de la PCA - Page Débogage», à la page 168.
- Pour plus d'informations, consultez les journaux de la PCA. Voir «Console Web de la PCA - Onglet Journaux de sauvegarde», à la page 159.

Console Web de la PCA - Onglet Console

La capture d'écran suivante indique les fonctions disponibles dans l'onglet **Console**, y compris les paramètres par défaut des quatre options de configuration :

Capture is On
Stop Click Stop to stop sending hits to the TeaLeaf appliance.
Capture is Enabled
Disable Click Disable to prevent the capture application from running at startup.
Web Console Time Out is Disabled
Enable Click Enable to start Web Console Timeout.
0 Set In minutes.

Figure 9. Onglet Console

Les options de l'onglet Console comprennent les options suivantes.

Paramètre
: **Description**

Démarrer/Arrêter la capture
: Ce bouton définit si le périphérique Passive Capture doit capturer les paquets du réseau. Lorsque ce paramètre est activé, les paquets sont capturés, et dans le cas contraire, ils ne le sont pas. Si cette option est désactivée, la capture ne peut pas démarrer.

Lorsque vous **arrêtez la capture**, la case à cocher **Réinitialiser toutes les statistiques avant de démarrer la capture** s'affiche.

Remarque : Si le basculement sur la machine maître/esclave de la PCA est activé, ne cochez pas la case **Réinitialiser toutes les statistiques avant de démarrer la capture** pour effacer les statistiques. Le fait d'effacer ou de réinitialiser les statistiques empêche le fonctionnement correct du basculement. Si l'effacement des statistiques est requis, arrêtez d'abord le basculement dans l'onglet correspondant. Le fait de redémarrer la PCA définit correctement l'état de basculement de la machine avec les statistiques effacées.

Activer/Désactiver capture
: Ce bouton contrôle le comportement de l'application de capture principale lorsque le service est démarré pendant le temps d'initialisation, à partir de la ligne de commande ou de la console Web. L'application de capture principale ne peut démarrer que lorsque cette option est activée.

Activer/Désactiver le délai d'attente de la console Web

Par défaut, la console Web de la PCA est configurée pour interrompre les sessions si aucune activité n'est détectée après 30 minutes.

- Pour désactiver le délai d'attente de la console, cliquez sur **Désactiver**.
  - Si l'authentification d'utilisateur pour la console Web est désactivée, il n'est pas possible d'appliquer de délai d'attente.
- Pour activer un délai d'attente, cliquez sur **Activer**. Saisissez une valeur non nulle correspondant au nombre de minutes pour le délai d'attente, puis cliquez sur **Définir**.
  - Les onglets automatiquement actualisés, comme les onglets Récapitulatif et Console, ne réinitialisent pas le délai d'attente.

    Remarque : il est possible d'activer ou de désactiver le délai d'attente de la console dans PCA Build 3600 ou supérieure.
    - Vous pouvez configurer la durée du délai d'attente de la console dans PCA Build 3500 ou supérieure. Cependant, il n'est pas possible de désactiver le délai d'attente de la console dans les builds antérieures à PCA 3600.

Console Web de la PCA - Onglet Interface

A partir de l'onglet **Interface**, vous pouvez configurer le nombre d'instances d'IBM Tealeaf Application de capture passive CX ainsi que les règles de trafic pour envoyer les données vers chaque instance.

Remarque : Vous pouvez configurer la console Web de la PCA de sorte qu'elle accepte par défaut des adresses IPv6. Voir «Navigateurs pris en charge pour la console Web de la PCA», à la page 54.

Remarque : Après l'enregistrement des modifications dans l'onglet **Interface**, redémarrez manuellement la PCA. Voir «Console Web de la PCA - Onglet Console» , à la page 70.

Application de capture passive CX peut être configurée pour prendre en charge l'équilibrage de charge transparent ou vous pouvez désactiver l'équilibrage de charge et utiliser la méthode existante permettant de capturer le trafic réseau. Pour plus d'informations sur les avantages de l'équilibrage de charge transparent, voir «Présentation de l'équilibrage de charge transparent de d'CX PCA», à la page 8. Pour configurer votre CX PCA de sorte qu'elle utilise l'équilibrage de charge transparent, voir «Configuration de l'interface PCA avec équilibrage de charge transparent», à la page 72. Si vous ne souhaitez pas activer l'équilibrage de charge transparent sur votre CX PCA, voir «Configuration de l'interface PCA sans équilibrage de charge transparent».

Configuration de l'interface PCA sans équilibrage de charge transparent



Figure 10. Sélectionner l'affichage

En haut de la page, vous pouvez sélectionner l'affichage.

- Pour configurer chaque instance d' IBM Tealeaf Application de capture passive CX, cliquez sur **Afficher les instances**. Voir «Affichage des instances», à la page 73.
- Pour modifier les filtres de données de chaque instance, cliquez sur **Modifier les filtres**. Voir «Modification des filtres», à la page 86.
- Pour consulter et modifier l'interface d'optimisation des paramètres, cliquez sur **Paramètres d'optimisation**. Voir «Paramètres d'optimisation», à la page 88.

Segmentation du trafic : par le biais de l'onglet Interface, vous pouvez segmenter le trafic vers plusieurs instances d'IBM Tealeaf Application de capture passive CX. Les deux méthodes suivantes sont disponibles pour la segmentation du trafic afin de répartir la charge :

- «Filtrage des adresses IP et de port de l'hôte du serveur Web», à la page 75

  Remarque : dans la mesure du possible, préférez la méthode de segmentation des adresses IP plutôt que celle des ports.
- «Filtrage de la segmentation du port TCP client», à la page 76
  - Voir «Segmentation du trafic», à la page 74.

Configuration de l'interface PCA avec équilibrage de charge transparent

Vous pouvez configurer l'interface réseau de votre Application de capture passive CX avec l'équilibrage de charge transparent. Pour plus d'informations sur les avantages de l'activation de l'équilibrage de charge transparent, voir «Présentation de l'équilibrage de charge transparent de d'CX PCA», à la page 8.

Pour configurer :

Dans l'onglet **Interface**, vous pouvez configurer le nombre d'instances d'IBM Tealeaf Application de capture passive CX et une règle de trafic pour l'envoi de données à chaque instance.

Remarque : Vous pouvez configurer la console Web de la PCA de sorte qu'elle accepte par défaut des adresses IPv6. Voir «Navigateurs pris en charge pour la console Web de la PCA», à la page 54.

Remarque : Après l'enregistrement des modifications dans l'onglet **Interface**, redémarrez manuellement la PCA. Voir «Console Web de la PCA - Onglet Console» , à la page 70.



Figure 11. Sélectionner l'affichage

En haut de la page, vous pouvez sélectionner l'affichage.

- Pour configurer chaque instance d' IBM Tealeaf Application de capture passive CX, cliquez sur **Afficher les instances**. Voir «Affichage des instances», à la page 73.
- Pour modifier les filtres de données de chaque instance, cliquez sur **Modifier les filtres**. Voir «Modification des filtres», à la page 86.

- Pour consulter et modifier l'interface d'optimisation des paramètres, cliquez sur **Paramètres d'optimisation**. Voir «Paramètres d'optimisation», à la page 88.

Segmentation du trafic : par le biais de l'onglet Interface, vous pouvez segmenter le trafic vers plusieurs instances d'IBM Tealeaf Application de capture passive CX. Les deux méthodes suivantes sont disponibles pour la segmentation du trafic afin de répartir la charge :

- «Filtrage des adresses IP et de port de l'hôte du serveur Web», à la page 75

  Remarque : dans la mesure du possible, préférez la méthode de segmentation des adresses IP plutôt que celle des ports.
- «Filtrage de la segmentation du port TCP client», à la page 76
  - Voir «Segmentation du trafic», à la page 74.

Affichage des instances

Les instances à interfaces multiples offrent à la PCA toutes les performances des processeurs multicoeurs en permettant à plusieurs processus de capturer simultanément du trafic réseau pour le rassemblement de hits HTTP et le déchiffrement SSL.

Figure 12. Instances

Remarque : le nombre d'instances PCA ne doit pas dépasser :
`(nombre de noyaux disponibles) - 1`
Voir Chapitre 2, «Installation», à la page 17.

- Pour activer la capture à partir de plusieurs instances, cochez la case correspondante.
- Pour désactiver la validation de total de contrôle des paquets capturés, cochez la case correspondante. Voir «Désactivation de la validation de total de contrôle des paquets», à la page 74.
- Pour ajouter une instance de la PCA, cliquez sur **Ajouter une instance**. Une instance est ajoutée à la liste des instances. Voir «Liste des instances», à la page 83.

- Afin de renseigner automatiquement les numéros de port pour les instances de la PCA en cours, cliquez sur **Renseigner les ports**. Voir «Renseignement des ports», à la page 76.
- Pour supprimer la totalité des filtres sur toutes les instances, cliquez sur **Supprimer les filtres**.

Désactivation de la validation de total de contrôle des paquets

Par défaut, la PCA effectue une validation de total de contrôle pour chaque paquet qui lui est transféré. Dans les environnements dont les cartes d'interface réseau (NIC) utilisent le système LRO (Large Receive Offload) ou le déchargement du total de contrôle (ou les deux), la validation de total de contrôle des paquets réseau capturés est gérée dans le matériel de la carte. Puisque la validation de total de contrôle est effectuée pour les paquets individuels dans le matériel, il n'est pas nécessaire d'effectuer un autre total de contrôle des paquets plus importants agrégés.

Lorsque l'une de ces options ou les deux sont activées, le total de contrôle des paquets transférés vers la PCA n'est pas recalculé. Par conséquent, le calcul du total de contrôle de la PCA échoue et le paquet est supprimé. Autres conséquences :

- Le nombre de pages manquantes ou partielles augmente dans les données de session
- Les statistiques de la PCA doivent signaler une augmentation importante dans `Total checksum errors`. Voir «Statistiques par instance», à la page 137.

Remarque : si la carte d'interface réseau utilisée par IBM Tealeaf Application de capture passive CX utilise le système LRO et/ou le déchargement du total de contrôle, vous devez désactiver la validation de total de contrôle dans la console Web de la PCA. Pour la désactiver, cochez la case `Disable Packet checksum validation` de l'onglet Interface.

Autrement, vous pouvez activer la validation de total de contrôle des paquets pour IBM Tealeaf Application de capture passive CX si vous désactivez le déchargement du total de contrôle par le biais du niveau pilote du système d'exploitation. Cependant, cette option ajoute une fonction de traitement au système d'exploitation.

- La commande permettant de désactiver le déchargement du total de contrôle dans la carte d'interface réseau doit être placée au début du script de configuration.

Segmentation du trafic

Les paquets capturés sont acheminés vers des instances individuelles de la PCA en fonction des paramètres du trafic souhaité pour chaque instance et ceux du trafic ignoré.

Passive Capture examine chaque paquet réseau et détermine le mode de trafic en fonction des règles de filtrage. A l'aide des filtres, vous pouvez spécifier la destination du trafic nécessaire, équilibrer la charge entre les instances de la PCA et définir les types de trafic que la PCA doit ignorer.

Remarque : la PCA configure automatiquement ses filtres d'écoute afin d'autoriser la capture des paquets VLAN 802.1q. Voir «Filtres VLAN», à la page 91.

- Pour supprimer la totalité des filtres sur toutes les instances, sélectionnez **Supprimer les filtres** dans la section Fonctions générales.

Vous pouvez configurer une des deux méthodes suivantes à partir de l'onglet Interface afin de répartir les charges entre plusieurs instances de la PCA :

- Filtrage des adresses IP et de port de l'hôte du serveur Web : la méthode la plus utilisée et conseillée pour la segmentation du trafic par une instance PCA est d'effectuer un filtrage sur les adresses IP et de port de l'hôte du serveur Web. Voir «Filtrage des adresses IP et de port de l'hôte du serveur Web».
- Filtrage par segmentation du port du client TCP : la méthode alternative, la segmentation du port du client TCP, est utilisée lorsque le trafic de capture se présente sous la forme d'une seule adresse IP virtuelle. Voir «Filtrage de la segmentation du port TCP client», à la page 76.

Filtrage des adresses IP et de port de l'hôte du serveur Web

Si le trafic de capture présenté à la PCA est fourni par plusieurs serveurs Web par le biais de leurs adresses IP et de port respectives, chaque instance de la PCA peut filtrer un sous-ensemble de ces adresses IP hôte. Cette méthode permet de distribuer les charges de trafic entre les instances.

Remarque : les filtres des adresses IP sont répertoriés dans l'ordre dans lequel vous les saisissez, et il n'est pas possible de modifier cet ordre de façon dynamique. Cependant, lorsque les filtres sont compilés au format binaire, ils peuvent être assemblés par adresse et par masque de réseau pour un traitement optimal, même si cela est peu probable. Consultez régulièrement la liste des filtres afin de vous assurer que tous les filtres actifs contiennent du trafic. Dans le cas contraire, les filtres doivent être supprimés de la liste.

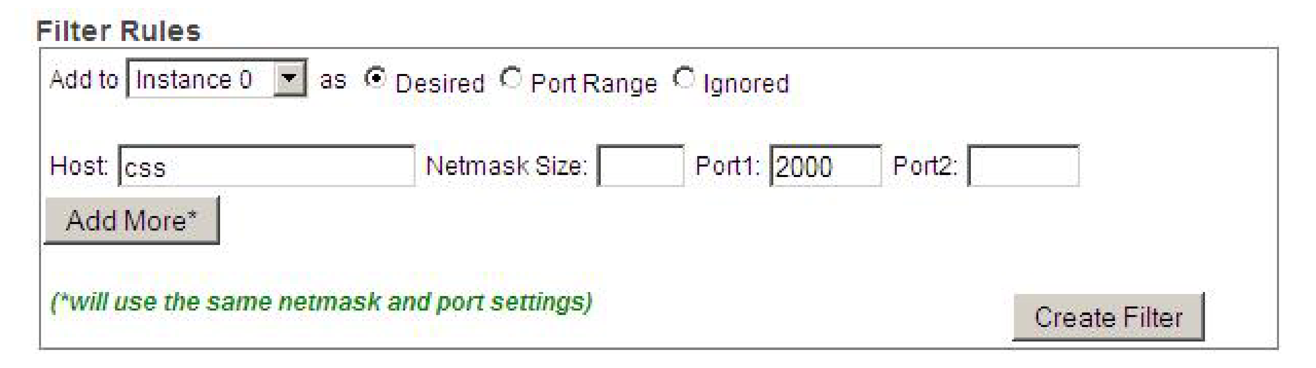


Figure 13. Règles de filtrage (PCA Build 35xx ou ultérieure)

Pour chaque instance de la PCA, les sections Liste des instances et Trafic ignoré identifient les paquets réseau à inclure et à exclure. Si le paquet correspond au trafic nécessaire et non au trafic à ignorer, capturez-le pour la suite du traitement.

- Voir «Règles de filtrage de trafic ignoré», à la page 81.

Dans la section Règles de filtrage, vous pouvez définir les adresses IP/ports qui transfèrent des données à la PCA. Vous pouvez ajouter et supprimer des adresses IP spécifiques ou une plage d'adresses IP. Vous pouvez également définir les hôtes spécifiques dont vous ne souhaitez pas que l'unité capture le trafic.

- Pour plus d'informations sur les meilleures pratiques de gestion des adresses IP, voir «Meilleures pratiques concernant les règles de filtrage», à la page 82.
- Pour plus d'informations sur la création de règles pour cette méthode de segmentation du trafic, voir «Règles de filtrage pour un hôte», à la page 78.
- Pour plus d'informations sur la création de règles afin d'ignorer le trafic, voir «Règles de filtrage de trafic ignoré», à la page 81.

Filtrage de la segmentation du port TCP client

Lorsque le trafic est fourni à partir d'une adresse IP virtuelle unique, vous pouvez utiliser la méthode de segmentation du port TCP client pour répartir le trafic selon des plages de ports TCP client.

Remarque : dans la mesure du possible, préférez la méthode de segmentation des adresses IP plutôt que celle des ports. Voir «Filtrage des adresses IP et de port de l'hôte du serveur Web», à la page 75.

Puisqu'il n'existe pas d'adresses IP de l'hôte du serveur Web à distribuer, la segmentation est effectuée par plage de ports TCP client. Chaque instance de la PCA filtre à partir d'une plage de ports TCP client. L'ensemble de toutes les plages de ports des instances de la PCA met en miroir la totalité du spectre des ports TCP client et assure par conséquent une capture complète.

Pour utiliser cette méthode :

- Le trafic de l'adresse IP virtuelle doit contenir uniquement le trafic de capture nécessaire. Tout le trafic de cette adresse IP virtuelle est utilisé.

  Remarque : assurez-vous que l'adresse IP virtuelle ne contient pas de trafic indésirable. Il est possible de définir une seule adresse pour ce type de filtrage.
- Les numéros de port TCP de l'hôte des serveurs Web doivent être inférieurs à 1024. Par exemple, les ports d'hôte 8443, 4443, et 1443 ne sont pas valides.
- Les règles de filtrage ignorées ne peuvent pas être utilisées.
- Pour plus d'informations sur la création de règles de filtrage pour cette méthode de segmentation du trafic, voir «Règles de filtrage pour une plage de ports», à la page 79.
- Pour plus d'informations sur la prise en charge des filtres personnalisés, contactez Tealeaf http://support.tealeaf.com.

Renseignement des ports

Remarque : l'utilisation de plages de ports pour segmenter le trafic capturé est une option avancée qui doit être définie uniquement lors de la configuration initiale d'IBM Tealeaf Application de capture passive CX. Pour toutes questions, contactez Tealeaf http://support.tealeaf.com.

Pour commencer, vous pouvez renseignez automatiquement les plages de ports dirigées vers chaque instance de la PCA. Toutes les plages à partir de 1024 sont réparties de manière équilibrée entre les instances de la PCA. Par exemple, si vous disposez de trois instances de la PCA, chacune reçoit le trafic provenant du même nombre de ports, qui correspond aux ports suivants :

```
(65,536 - 1024) / 3 = 21,504 ports/instance
```

Remarque : les numéros de port valides sont compris entre 1024 et 65,535. Les numéros de port inférieurs à 1024 sont réservés.

- Pour plus d'informations, voir `http://www.iana.org/assignments/port-numbers`.

Remarque : lorsque les ports sont renseignés automatiquement, tous les autres filtres d'écoute des instances de la PCA sont supprimés.

1. Pour renseigner les plages de ports, cliquez sur **Renseigner les ports**.
2. Les plages de ports sont renseignées pour toutes les instances de la PCA disponibles. Enregistrez vos modifications.

3. Redémarrez la PCA.

Après avoir renseigné les ports, contrôlez la charge du trafic envoyée vers chaque instance. Par exemple, supposons que votre serveur Web distribue des réponses HTTP sur le port 8080. L'instance de la PCA recevant le trafic peut alors fonctionner au maximum alors que les autres sont peu utilisées.

Les statistiques des hits Current par seconde sont disponibles dans l'onglet Récapitulatif, et chaque instance de la PCA est rapportée sous une valeur d'ID distincte.

- Le débit de hits SSL/s est rapporté dans la colonne Hits SSL de reassd.
- Le débit des hits non-SSL/s est rapporté dans la colonne Hits non-SSL.

Voir «Console Web de la PCA - Onglet Récapitulatif», à la page 60.

Ajustements

- Si des déséquilibres sont présents, pensez à appliquer des règles de filtrage supplémentaires.
- Sur les serveurs d'IBM Tealeaf Application de capture passive CX multicoeurs, vous pouvez créer plusieurs instances de la PCA et répartir la charge sur toutes les plages de ports configurables. Voir «Equilibrage de la charge entre les instances de la PCA à l'aide des plages de ports».
- Après avoir renseigné automatiquement les ports, vous pouvez configurer une adresse IP virtuelle. Voir «Modification des règles de filtrage de plage de ports existantes», à la page 81.

Equilibrage de la charge entre les instances de la PCA à l'aide des plages de ports

Lorsque vous renseignez les plages de ports de toutes les instances de la PCA, cette dernière affecte le même nombre de ports à chacune de ses instances disponibles. Cependant, en règle générale, l'infrastructure réseau de l'entreprise ne distribue pas la charge du trafic de manière équilibrée dans la plage de ports disponibles. Après avoir renseigné les plages de ports, vous remarquerez que la charge du trafic n'est pas distribuée de manière équilibrée entre les instances. Par exemple, l'instance 0 de la PCA peut traiter 75 % des données transférées, alors que l'instance 1 de la PCA traite seulement 25 %, même si chaque instance est en mode écoute sur le même nombre de ports.

Les étapes suivantes vous permettent d'ajuster les plages de ports affectées à chaque instance de la PCA afin d'équilibrer la charge entre les instances disponibles. Ce processus peut nécessiter des réglages et une personnalisation itératifs et entraîner des pics de trafic.

1. Instanciez le nombre nécessaire d'instances de la PCA. Voir «Affichage des instances», à la page 73.
2. Dans l'onglet Interface, cliquez sur **Renseigner les ports**.
3. Enregistrez vos modifications.
4. Cette étape permet de distribuer la charge du trafic de manière équilibrée sur tous les ports. Les étapes suivantes doivent être répétées jusqu'à ce que la charge du trafic soit distribuée de manière équilibrée sur tous les ports des instances de la PCA :
   a. Vérifiez le nombre de hits SSL/sec traités par chaque instance. Le traitement des hits SSL est l'opération qui sollicite le plus le processeur et constitue un indicateur fiable pour l'équilibrage de charge. Si les hits SSL ne représentent

pas le volume de trafic principal, utilisez le débit de hits non-SSL/sec pour évaluer la charge. Si nécessaire, vous pouvez utiliser les deux.

- Les statistiques concernant les hits Current par seconde sont rapportées dans l'onglet Récapitulatif, et chaque instance de la PCA est représentée par une valeur d'ID distincte.
- Le débit de hits SSL/sec est rapporté dans la colonne Hits SSL de reassd.
- Le débit des hits non-SSL/sec est rapporté dans la colonne Hits non-SSL.
- Voir «Console Web de la PCA - Onglet Récapitulatif», à la page 60.

b. En fonction des débits de hits par seconde de chaque instance de la PCA, modifiez et personnalisez les plages de ports, en les élargissant ou en les réduisant au besoin, dans le but d'équilibrer au mieux la charge.

c. Ajustez et contrôlez les résultats dans l'onglet Récapitulatif.

Remarque : la console Web de la PCA ne valide pas les plages de ports spécifiées. Vérifiez pour chaque ajustement qu'aucun écart ou chevauchement n'est créé dans les plages de ports et que la totalité de la plage des ports disponibles n'est pas spécifiée.

d. Il est peu probable qu'un ensemble d'ajustements donne lieu à une distribution équilibrée. Dans la mesure où les débits de charge peuvent varier avec le temps, il serait suffisant de maintenir les débits de hits/s pour chaque plage à 25 %.

e. Enregistrez vos modifications. La PCA redémarre automatiquement et les modifications sont appliquées.

f. Répétez ces étapes jusqu'à ce que la charge soit équilibrée à votre convenance.

5. Lorsque vous avez terminé vos ajustements, vérifiez que la totalité de la plage des ports disponibles (1024 - 65535) est couverte par votre ensemble de plages de ports. Les écarts et les chevauchements doivent être éliminés.

Règles de filtrage

Vous pouvez utiliser des règles de filtrage pour filtrer les paquets de données entrants et les transférer vers des instances de la PCA définies. Il est possible de définir des règles pour filtrer en fonction du nom d'hôte, du masque de réseau et de la plage de ports du trafic entrant.

Remarque : Le panneau Règles de filtrage permet d'ajouter une règle de filtrage unique à appliquer à plusieurs hôtes sur plusieurs instances de la PCA. Lors de la création et du débogage initiaux, la vue Modifier les filtres propose des méthodes plus simples afin de vérifier si les ports sont couverts par vos règles de filtrage sur toutes les instances. Voir «Modification des filtres», à la page 86.

Règles de filtrage pour un hôte

Il est possible d'utiliser des règles de filtrage sur un hôte pour acheminer le trafic nécessaire ou ignoré en fonction de l'hôte qui l'envoie.

- Utilisez un filtre de plage de ports pour définir le trafic basé sur les ports. Voir «Règles de filtrage pour une plage de ports», à la page 79.

Pour définir une règle de filtrage pour un hôte :

Remarque : ne mélangez pas les règles de filtrage de deux méthodes de segmentation du trafic. Vous pouvez uniquement utiliser les règles de filtrage définies pour la méthode sélectionnée.

1. Saisissez l'adresse IP de l'hôte.

- Si cette valeur n'est pas indiquée, toutes les adresses IP de l'hôte sont capturées à partir des numéros de port spécifiés. Cependant, le paramètre de taille du masque de réseau ne peut pas être utilisé sans une valeur valide pour l'hôte.
- Pour ajouter un hôte, cliquez sur **Ajouter**.
  - Dans PCA Build 34xx et antérieure, cliquez sur le lien **Ajouter un hôte**.

2. Si le trafic de l'hôte provient d'un masque de réseau spécifique, saisissez la valeur ici.
3. Si les zones Port1 et Port2 ne sont pas renseignées, tout le trafic de l'hôte ou du masque de réseau est filtré selon la règle. Dans le cas d'une règle basée sur l'hôte, n'indiquez pas de ports spécifiques.
4. A partir du menu déroulant Ajouter à, sélectionnez l'instance de la PCA à laquelle la règle doit s'appliquer.
5. Sélectionnez ensuite le type de règle de filtrage :
   - `Desired` : le trafic spécifié est transféré vers l'instance sélectionnée.
   - `Ignored` : le trafic spécifié est ignoré et supprimé pour la suite du traitement. Voir «Règles de filtrage de trafic ignoré», à la page 81.
6. Cliquez sur **Ajouter**.
7. La règle de filtrage est ajoutée à l'instance spécifiée et s'applique immédiatement au trafic entrant.

Règles de filtrage pour une plage de ports

Il est possible d'utiliser une règle de filtrage pour une plage de ports afin d'acheminer le trafic nécessaire via un ensemble de ports spécifié vers une instance de la PCA. Vous pouvez spécifier des filtres pour une plage de ports à l'aide des méthodes prises en charge suivantes :

Remarque : les numéros de port valides sont compris entre 1024 et 65,535.

Remarque : n'utilisez pas les règles de filtrage des deux méthodes de segmentation du trafic. Vous pouvez uniquement utiliser les règles de filtrage définies pour la méthode sélectionnée.

- Automatique : la méthode recommandée afin de spécifier des filtres pour les plages de ports est de renseigner automatiquement les ports. Elle permet de créer à votre place la règle de filtrage adaptée pour la plage de ports. Cela suppose que toutes les instances nécessaires sont déjà créées. Voir «Renseignement des ports», à la page 76.
  - Si nécessaire, vous pouvez modifier les plages de ports après qu'elles ont été renseignées automatiquement. Voir «Modification des règles de filtrage de plage de ports existantes», à la page 81.
- Manuelle : si vous spécifiez manuellement les plages de ports (non renseignées automatiquement), seule une entrée d'adresse IP est autorisée pour le filtrage des adresses IP virtuelles. Toute adresse IP supplémentaire ajoutée aux plages de ports sera ignorée.
  - Vous pouvez utiliser un masque de sous-réseau avec une adresse IP unique comme alternative.
  - Les étapes suivantes vous permettront de spécifier manuellement une règle de filtrage d'une plage de ports pour les instances spécifiées.
  - Si vous devez modifier des règles existantes, cliquez sur **Modifier les filtres** dans l'onglet Interface.

Les règles de filtrage d'une plage de ports peuvent filtrer sur une adresse IP virtuelle, ce qui permet de filtrer le trafic indésirable à l'aide du trafic de l'adresse IP virtuelle.

- Il n'est pas nécessaire d'indiquer une adresse IP ici si le trafic de capture contient uniquement le trafic nécessaire.

Ajout ou spécification d'une règle de filtrage pour une plage de ports manuel :

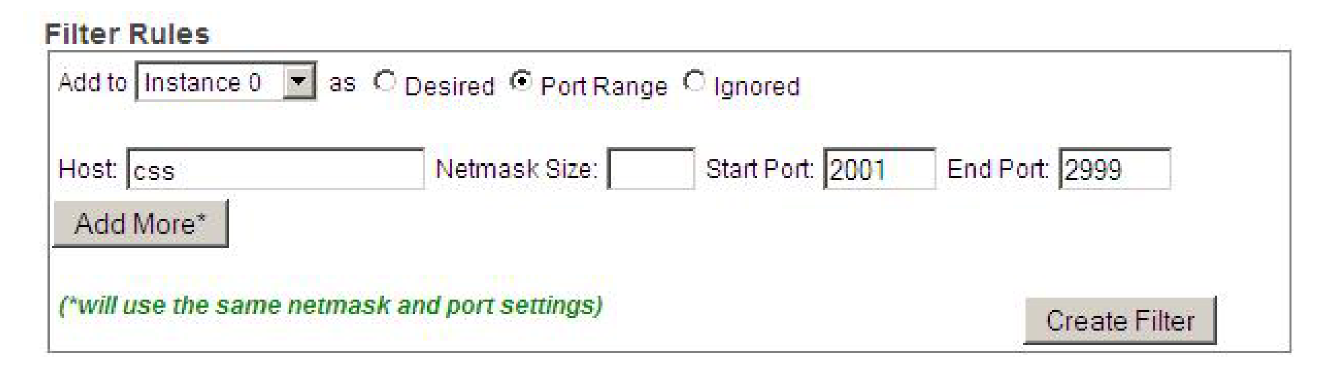


Figure 14. Ajout manuel de règles de filtrage pour une plage de ports (PCA Build 35xx ou supérieure)

1. Si nécessaire, sous Règles de filtrage saisissez l'adresse IP de l'adresse virtuelle dans la zone `Host`.
2. Pour le type de règle de filtrage, sélectionnez `Port Range` qui envoie le trafic spécifié vers l'instance sélectionnée.
3. Utilisez la même adresse IP pour chaque règle de filtrage de plage de ports.
   - Si plusieurs adresses IP sont nécessaires et sont regroupées dans un sous-réseau, vous pouvez appliquer un masque de sous-réseau à l'adresse IP de base. Par exemple, l'entrée `66.211.169.0/24` correspond aux 24 premiers bits de l'adresse IP (les trois premiers octets) et permet une correspondance générique sur une valeur du quatrième octet, défini à `0`. Chaque plage de ports spécifiée pour cette adresse IP virtuelle correspond aux 254 adresses IP de l'adresse virtuelle.
4. Si le trafic de l'adresse IP virtuelle provient d'un masque de réseau spécifique, saisissez ici la valeur du masque.
5. Indiquez la valeur du port de début dans la zone `Start Port` et la valeur du port de fin dans la zone `End Port`.
6. A partir du menu déroulant Instance, sélectionnez l'instance de la PCA à laquelle appliquer la règle.
7. Cliquez sur **Créer filtre**.
   - Dans PCA 34xx et version antérieure, cliquez sur **Ajouter**.
8. La règle de filtrage est ajoutée à l'instance spécifiée et s'applique immédiatement au trafic entrant.

   Remarque : une seule règle de filtrage de plage de ports doit être ajoutée à chaque instance. Toute règle supplémentaire sera ignorée.

   Remarque : Après l'enregistrement des modifications dans l'onglet Interface, redémarrez manuellement la PCA. Voir «Console Web de la PCA - Onglet Console», à la page 70.

Modification des règles de filtrage de plage de ports existantes :

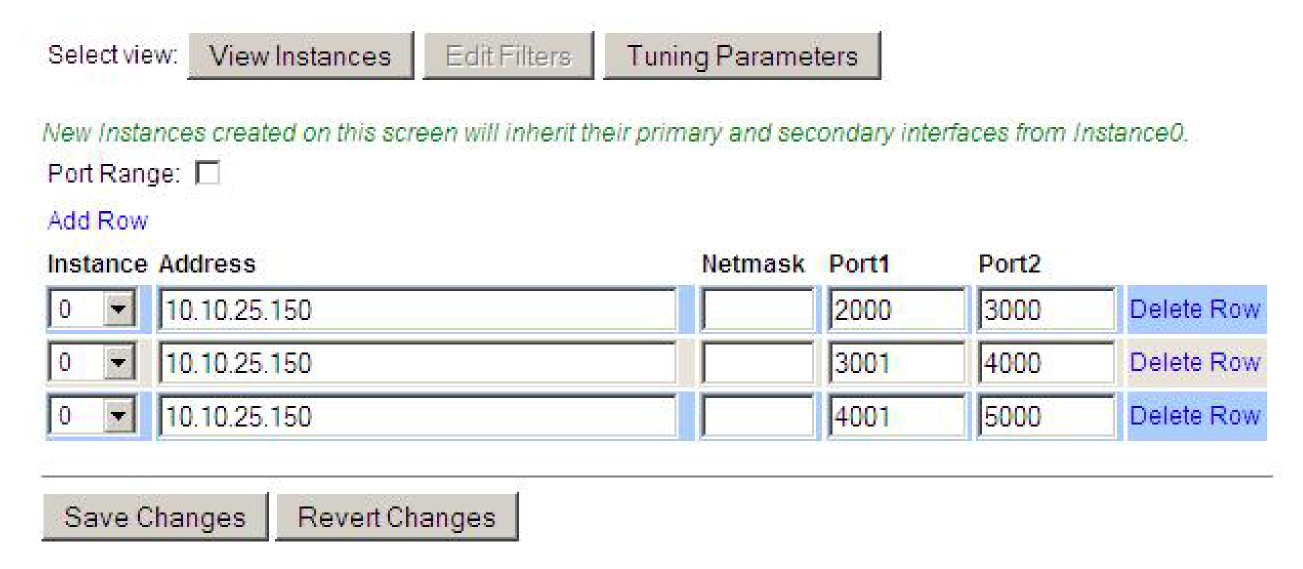


Figure 15. Modification des règles de filtrage de plage de ports existantes à l'aide d'une adresse IP virtuelle

Remarque : Vous pouvez utiliser ce mode pour ajouter une adresse IP virtuelle lorsque l'option de remplissage automatique des données de ports est activée (bouton Renseigner les ports).

1. Si nécessaire, sur l'écran Modifier les filtres, cochez la case **Plage de ports**.
2. Saisissez l'adresse IP de l'adresse virtuelle dans la zone `Adresse`.
3. Utilisez et appliquez la même adresse IP pour chaque règle de filtrage de plage de ports.
4. Modifiez au besoin les zones des règles de filtrage.
5. Pour appliquer les modifications, cliquez sur **Enregistrer les modifications**.

   Remarque : Après l'enregistrement des modifications dans l'onglet **Interface**, redémarrez manuellement la PCA. Voir «Console Web de la PCA - Onglet Console», à la page 70.
6. Les modifications de la configuration sont appliquées au trafic entrant.

Règles de filtrage de trafic ignoré

Vous pouvez définir des règles de filtrage afin d'ignorer le trafic. Ces règles s'appliquent à toutes les instances de la PCA.

Ignored Traffic (Global)

Host 10.10.25.255	x
Port 4000	x
Port 4001	x
Host 10.10.25.254 and Port 4002	x

Figure 16. Définition d'une règle de filtrage de trafic ignoré

1. Définissez la règle dans la zone Règles de filtrage.

a. Indiquez l'hôte à partir duquel vous souhaitez ignorer le trafic. Pour ignorer la totalité du trafic à partir d'une valeur de port spécifique, ne renseignez pas cette valeur.
b. Si nécessaire, spécifiez le port à ignorer. Pour ignorer la totalité du trafic de l'hôte, n'indiquez pas le masque de réseau ni les valeurs de port.

   Remarque : vous ne pouvez pas définir de plages de ports pour les règles de trafic ignoré.
2. Cochez la case **Ignoré**.
3. Cliquez sur **Créer filtre**.
   - Dans PCA 34xx et antérieure, cliquez sur **Ajouter**.
4. La règle est insérée dans la zone Trafic ignoré (Global) située au bas de l'écran.

Ignored Traffic (Global)

Host 10.10.25.255	x
Port 4000	x
Port 4001	x
Host 10.10.25.254 and Port 4002	x

Figure 17. Trafic ignoré (Global)

Tout le trafic envoyé à partir des adresses correspondant aux règles de trafic ignoré est supprimé de la PCA.

Meilleures pratiques concernant les règles de filtrage

Nous vous recommandons de limiter à 20 le nombre de règles de filtrage pour chacune des instances de la PCA.

Remarque : plus il y a d'entrées, moins le filtrage des adresses IP est efficace, c'est pourquoi nous vous recommandons de limiter à 20 le nombre d'entrées par instance.

Pour résoudre ce problème, vous pouvez :
- Réduire le nombre de règles de filtrage à l'aide de masques de sous-réseau. Par exemple, si vous avez défini des règles de filtrage individuelles pour chaque port d'une plage, utilisez un masque de sous-réseau pour créer une règle de filtrage unique pour tous les ports.
- Créer plusieurs instances de l'application PCA. Voir Chapitre 2, «Installation», à la page 17.

Association de filtres pour des adresses IP et des plages de ports spécifiques

Vous pouvez utiliser des combinaisons d'adresses IP et de plages de ports spécifiques pour filtrer le trafic.

Remarque : la méthode de configuration du filtre est disponible uniquement pour les utilisateurs avancés de la PCA. Elle n'est pas prise en charge par l'interface de la console Web de la PCA et peut être uniquement effectuée en modifiant manuellement le fichier de configuration. Après avoir utilisé cette méthode, vous ne pouvez plus modifier vos filtres par le biais de la console Web.

Remarque : si vous associez ces méthodes, il se peut que le trafic soit dupliqué lorsque vous modifiez manuellement ce fichier.

Pour associer des modes de filtrage dans une même configuration, vous devez insérer des entrées dans le fichier `ctc-conf.xml` selon l'exemple suivant :

Remarque : il est possible que les entrées modifiées manuellement soient supprimées si vous utilisez la console Web de la PCA et qu'elles modifient sa configuration.

```
<Instance>
                <ListenTos>
                    <ListenTo>
                        <Address>10.10.100.200</Address>
                        <PortRange>33280-65535</PortRange>
                    </ListenTo>
                </ListenTos>
            </Instance>
```

Voir «Fichier de configuration Passive Capture `ctc-conf.xml`», à la page 171.

Liste des instances

Instance List

Instance 0 (primary) edit | clear filters

Primary Interface:	eth0: up	Listen Interface:	both	
Secondary Interface:	eth4: up	Listen Direction:	Unidirectional	
Desired Traffic	Port 80 or 443			x

Instance 1 (enabled) edit | clear filters | delete

Primary Interface:	eth1: up	Listen Interface:	both	
Secondary Interface:	eth2: up	Listen Direction:	Unidirectional	
Desired Traffic	Port 80 or 443			x

Figure 18. Instances

Dans la liste des instances, vous pouvez configurer, activer désactiver et supprimer des instances d'IBM Tealeaf Application de capture passive CX sur le serveur.

- Pour supprimer une instance créée, cliquez sur le lien Supprimer en face de son nom dans la liste des instances.
  - Vous ne pouvez pas supprimer l'instance principale.
- Pour basculer vers une instance secondaire, cliquez sur le lien Activé ou Désactivé à côté de son nom.
- Pour supprimer tous les filtres d'une instance spécifique, cliquez sur **Supprimer les filtres**.
- Pour modifier une instance, cliquez sur le lien Modifier en face de son nom. Voir «Interfaces réseau de capture», à la page 84.

Interfaces réseau de capture

Settings for Instance 0

Primary Interface: eth0: up

Secondary Interface: eth4: up

Listen Interfaces: Both interfaces / Primary interface only / Inherited from Primary

Listen Direction: Bidirectional / Unidirectional / Inherited from Primary

Update

Figure 19. Interfaces réseau de capture

Vous trouverez ci-dessous la description des options affichées dans la capture d'écran.

Remarque : si vous utilisez plusieurs instances, elles doivent toutes être configurées dans la liste de l'instance principale. Dans le cas contraire, la PCA ne démarrera pas.

Paramètre
: **Description**

`Interface principale`
: Ce menu déroulant désigne une interface réseau matérielle spécifique comme interface principale pour la capture. Il s'agit d'une liste dynamique des interfaces importantes.

`Interface secondaire`
: Ce menu déroulant désigne une interface réseau matérielle spécifique comme interface secondaire pour la capture. Il s'agit d'une liste dynamique des interfaces importantes.

`Interface d'écoute`
: Définit les interfaces sur lesquelles l'instance sélectionnée est en mode écoute :

- `Both Interfaces` : les deux interfaces écoutent le trafic.
- `Primary Interface only` : seule l'interface principale écoute le trafic.
- `Inherited from Primary` : les interfaces d'écoute sont héritées de l'instance principale.

`Direction d'écoute`
: Indique le sens dans lequel les interfaces sélectionnées écoutent le trafic :

- `Bidirectional` : les interfaces sélectionnées écoutent les paquets entrants et sortants.
- `Unidirectional` : l'interface principale écoute les paquets entrants et l'interface secondaire se charge des paquets sortants.
- `Inherited from Primary` : le sens d'écoute est hérité de l'instance principale.

Exemples

Vous trouverez ci-dessous des exemples d'interfaces.

Interface principale uniquement bidirectionnelle

Cette option permet d'écouter les paquets entrants et sortants à partir de l'interface principale. Utilisez-la lorsque vous êtes connecté à un seul segment de réseau par le biais d'un commutateur avec un port miroir ou d'un hub.

Interfaces principale et secondaire bidirectionnelles

Cette option permet d'écouter les paquets entrants et sortants à partir des deux interfaces. Utilisez-la lorsque vous êtes connecté à deux segments de réseaux séparés par le biais de commutateurs avec un port miroir ou de concentrateurs.

Interfaces principale et secondaire unidirectionnelles

Cette option permet d'écouter les paquets entrants à partir de l'interface principale et les paquets sortants à partir de l'interface secondaire. Utilisez-la lorsque vous êtes connecté à un seul segment de réseau par le biais d'un tap réseau.

Trafic à ignorer

Cette section indique le trafic que l'unité doit ignorer de manière explicite. Même si une paire hôte-port de cette liste remplit le critère de la section Trafic nécessaire, l'unité ne la capture pas. Pour ignorer la totalité du trafic d'un hôte, saisissez `*` ou `All` à la place du numéro de port.

Lorsque vous spécifiez des combinaisons d'hôtes et de ports à ignorer, vous ajoutez des restrictions correspondant à des paquets ne devant pas faire partie des combinaisons d'hôtes et de ports. Par exemple, vous souhaitez capturer la totalité du trafic entrant et sortant des hôtes qui communiquent sur les ports 1, 2, et 3 sauf pour les combinaisons d’hôtes et de ports suivantes :

Hôte	Port
1.2.3.4	4
5.6.7.8	5

La description de ce trafic est identique à l'exécution de la commande unique suivante :

```
tcpdump -n -i eth0 "((port 1) or (port 2) or (port 3)) and not \
((host 1.2.3.4 and port 4) or (host 5.6.7.8 and port 5))"
```

Dans le fichier `ctc-conf.xml`, l'exemple ci-dessus correspond au langage XML suivant :

```
<Ignores>
    <Ignore>
        <Address>1.2.3.4</Address>
        <Port>4</Port>
    </Ignore>
    <Ignore>
        <Address>5.6.7.8</Address>
        <Port>5</Port>
    </Ignore>
</Ignores>
<ListenTos>
    <ListenTo>
        <Port>1</Port>
```

```
    </ListenTo>
    <ListenTo>
        <Port>2</Port>
    </ListenTo>
    <ListenTo>
        <Port>3</Port>
    </ListenTo>
</ListenTos>
```

Modification des filtres

Dans la vue Modifier les filtres, vous pouvez modifier les ports et les plages de ports pour filtrer les données envoyées à chaque instance de la PCA. Utilisez cette vue pour vous assurer que toutes les plages de ports sont correctement spécifiées pour toutes les instances d'IBM Tealeaf Application de capture passive CX.

- Vous pouvez également définir des filtres de données dans la vue Afficher les instances. Voir «Règles de filtrage», à la page 78.

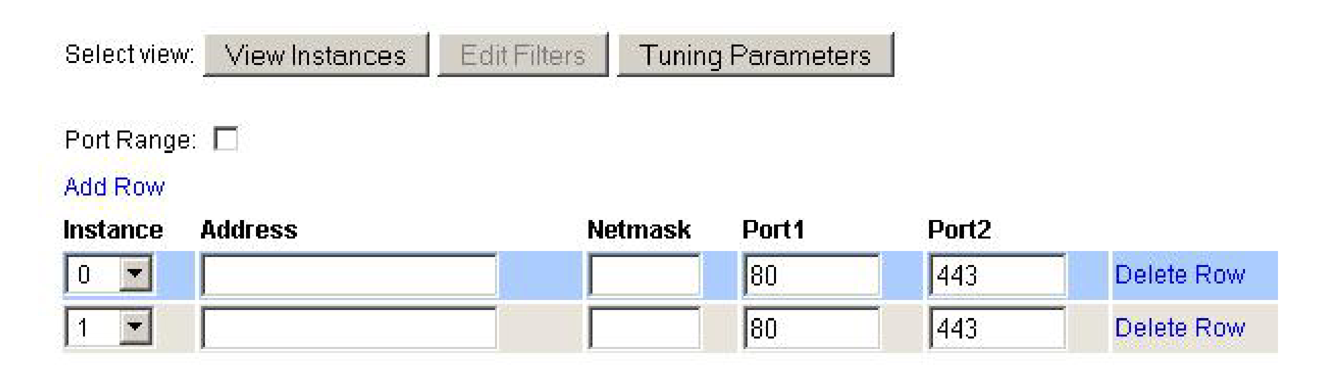


Figure 20. Modifier les filtres

Par défaut, la vue Modifier les filtres permet de spécifier un maximum de deux ports individuels auxquels envoyer des données pour une PCA individuelle.

- Pour spécifier une plage de ports, cochez la case **Plage de ports**. Les données de la case à cocher du port deviennent une plage de début et de fin pour la capture et le transfert.
- Pour ajouter une ligne, cliquez sur le lien **Ajouter une ligne**. Une nouvelle ligne s'insère.
- Pour supprimer une ligne de filtre de données, cliquez sur le lien **Supprimer une ligne**.

Pour définir un filtre de données :

1. Dans la colonne Instance, sélectionnez l'identificateur de l'instance de la PCA à laquelle appliquer le filtre. Toutes les données capturées du serveur et des ports spécifiés sont transférées vers l'instance sélectionnée.
   - Voir «Liste des instances», à la page 83.
2. Dans la colonne Adresse, saisissez l'adresse IP du serveur qui fournit les données.

   Remarque : les noms d'hôte ne sont pas acceptés.
3. Dans la colonne Masque de réseau, vous pouvez saisir un masque de réseau, le cas échéant.
4. Indiquez les ports à capturer :

- Si la case Plage de ports n'est pas cochée, vous pouvez spécifier un maximum de deux ports à capturer à partir de l'adresse indiquée.
- Si la case Plage de ports est cochée, vous pouvez indiquer un port de début et un port de fin dans les deux zones de texte. Ces entrées indiquent une plage de ports qui seront transférés à l'instance PCA sélectionnée pour la capture.

Format CIDR

Utilisez le format CIDR pour configurer un bloc d'adresses IP admissibles. Ce format spécifie une plage d'adresses IP en associant une adresse IP et son masque de réseau. La notation CIDR utilise le format suivant :

```
192.30.250.00/18
```

- Dans cet exemple, `192.30.250.00` représente l'adresse réseau. 18 indique que les 18 premiers octets correspondent à la partie réseau de l'adresse ; les 14 derniers octets peuvent être utilisés pour des adresses hôtes spécifiques.

Consultez le tableau suivant pour plus d'exemples :

Format CIDR	Masque de réseau équivalent
10.10.0.0/16	255.255.0.0
10.10.10.0/24	255.255.255.0
10.10.10.0/28	255.255.255.240

Trafic du miroir de port

Si vous capturez un sous-réseau à partir d'un miroir de port, vous devez déterminer si ce dernier doit vous transmettre uniquement le trafic de ce sous-réseau ou un autre.

Si vous recevez uniquement le trafic du sous-réseau, sélectionnez **Ports spécifiques sur tous les hôtes** afin de capturer des ports spécifiques. Par exemple, pour capturer le trafic des ports 80 et 443 sur tous les hôtes, sélectionnez **Ports spécifiques sur tous les hôtes** et indiquez les ports `80` et `443`.

Si votre miroir de port copie du trafic supplémentaire, sélectionnez **Combinaisons hôte-port spécifiques**. Pour les hôtes, utilisez la syntaxe CIDR afin qu'ils correspondent au sous-réseau. Si, en gardant l'exemple des ports 80 et 443, vous souhaitez capturer le trafic du réseau 1.2.3.0 masque de réseau 255.255.255.0, indiquez les combinaisons hôte-port spécifiques suivantes :

Hôte	Port
1.2.3.0/24	80
1.2.3.0/24	443

Paramètres d'optimisation

La section Paramètres d'optimisation définit les caractéristiques des performances du système.

Select view: View Instances | Edit Filters | Tuning Parameters

Tuning Parameters

Max input buffer size	100	MB (between 1 and 10000)
Max memory consumption	1300	MB (default=1300)
Max simultaneous connections	10000	(default=10,000)
Max simultaneous connections in SYN state	4000	(default=5000)
Max SSL sessions to cache	10000	(default=10000)
Max wait time for hit responses	300	seconds (default=120)
Max wait time for hit transmissions	300	seconds (default=120)
Max large capture packet size	8	kB (default=8)

Save Changes | Revert Changes

Figure 21. Paramètres d'optimisation (paramètres de la capture)

Voici la description des options affichées dans la capture d'écran ci-dessus :

Paramètre
Description

`Taille maximale de la mémoire tampon d'entrée`
Permet de définir la taille de la mémoire tampon entre le renifleur de paquets et l'assembleur de hits. Si l'assembleur de hits est trop lent, les paquets sont placés en file d'attente dans cette mémoire tampon afin d'être traités. Lorsque les ressources de l'assembleur de hits sont disponibles, il est en mesure d'extraire les paquets de la file d'attente et de les traiter.

- Quand la mémoire tampon se remplit, la PCA commence à abandonner les hits. La limite de la mémoire tampon permet d'éviter que le système ne tombe en panne, cependant, certaines données sont supprimées.

  Remarque : Tealeaf vous recommande de conserver la valeur par défaut de ce paramètre. Il est utilisé pour déboguer les problèmes liés aux pics de trafic entraînant une surcharge de la mémoire tampon. Ne modifiez pas ce paramètre sans l'avis de Tealeaf.

`Consommation maximale de mémoire`
Permet de définir la quantité maximale de mémoire système(en Mo) allouée au processus de capture. La valeur par défaut est fixée à `1300` (environ 1,3 Go).

- IBM Tealeaf Application de capture passive CX est une application 32 bits, par conséquent chaque processus de la PCA peut gérer un maximum de 2 Go de mémoire RAM.

Remarque : Tealeaf vous recommande de conserver la valeur par défaut de ce paramètre. Il est utilisé pour déboguer les problèmes liés aux volumes de trafic croissants entraînant une surcharge de la PCA. Ne modifiez pas ce paramètre sans conseils de Tealeaf.

Nombre maximal de connexions simultanées
Permet de définir le nombre maximal de connexions TCP sur lesquelles le système peut effectuer une capture simultanée. Si le nombre de connexions est supérieur à ce nombre, le système de capture remplace les anciennes connexions par les nouvelles. Après la fermeture d'une ancienne connexion, le système commence la capture pour la nouvelle connexion suivante. Ainsi, le système empêche un trop grand nombre de connexions entraînant une surcharge des ressources système de causer une panne.

Remarque : ce paramètre s'applique à chaque instance de la PCA. S'il fait partie de l'installation initiale ou d'une mise à niveau de la PCA, ce paramètre doit être modifié en fonction du volume du trafic actuel. Voir Chapitre 2, «Installation», à la page 17.

Nombre maximal de connexions en état SYN
Permet de définir le nombre maximal de connexions TCP simultanées dont l'état est SYN. Si le nombre de connexions pour cet état est supérieur au nombre défini, le système remplace les anciennes connexions par les nouvelles. Une fois qu'un ancienne connexion se ferme ou passe à un autre état, le système commence la capture pour la nouvelle connexion suivante. Ainsi, le système empêche les attaques SYN de causer une panne.

Remarque : ce paramètre s'applique à chaque instance de la PCA. S'il fait partie de l'installation initiale ou d'une mise à niveau de la PCA, ce paramètre doit être modifié en fonction du volume du trafic actuel. Voir Chapitre 2, «Installation», à la page 17.

Nombre maximal de sessions SSL à mettre en cache
Permet de définir le nombre maximal de sessions SSL que le système peut mettre en mémoire cache simultanément. Une fois que le système a atteint cette limite, il supprime les entrées les plus anciennes en premier. Si une session correspondant à une entrée supprimée reprend, le système n'est pas en mesure de la décoder. Ainsi, le système empêche un trop grand nombre de sessions n'ayant pas été terminées correctement de causer une panne.

- il est possible d'augmenter ce paramètre sous certaines contraintes. Pour plus d'informations, voir section "Traitement des incidents - Capture" du *Guide de dépannage d'IBM Tealeaf*.

Temps d'attente maximal pour les réponses aux hits
Permet de définir la durée du minuteur utilisé pour déterminer si un serveur est bloqué sur une demande HTTP. Une fois que le système reçoit le dernier paquet d'une demande, il lance le minuteur. Si ce dernier expire avant d'avoir reçu le premier paquet de la réponse, le système identifie la demande comme étant bloquée et la place dans un paquet en tant que hit bloqué. Finalement, si la réponse arrive, le système l'ignore. En imposant ce minuteur, le système évite que les demandes bloquées utilisent les ressources.

Temps d'attente maximal pour les transmissions de hits
Permet de définir la durée du minuteur utilisé pour déterminer si une connexion TCP est suspendue. Le minuteur démarre une fois que le système a reçu un paquet pour une connexion. Si le minuteur expire avant

de recevoir un autre paquet, le système identifie la connexion comme suspendue et l'annule. Si la connexion correspond à une demande HTTP, le système l'ignore totalement. Si elle correspond à une réponse HTTP, le système place les données de la réponse partielle dans un hit. En imposant ce minuteur, le système évite que les connexions suspendues utilisent les ressources.

Taille maximale des grands paquets de capture
Permet de définir la taille maximale pour la capture des paquets TCP. La valeur par défaut est de 8 Ko.

Modification manuelle de la configuration de l'interface

La plupart du temps, vous pouvez définir une configuration pour l'interface dans la console Web de la PCA Il peut, dans de rares cas, être nécessaire d'effectuer des modifications manuelles dans la configuration de l'interface par le biais du fichier `ctc-conf.xml`.

Paramètre
Description

All Traffic
Cette option permet de capturer tous les paquets vers ou à partir d'un hôte du segment de réseau. Lorsque vous choisissez de capturer tout le trafic nécessaire, la description est une instruction vide correspondant à tous les paquets TCP/IP possibles. Cela produit le même effet que l'exécution de cette commande :

```
tcpdump -n -i eth0
```

Dans le fichier `ctc-conf.xml`, le langage XML suivant indique qu'il est nécessaire de capturer la totalité du trafic :

```
<ListenTos>
    <ListenTo>*</ListenTo>
</ListenTos>
```

Specific Ports on All Hosts
Cette option permet de capturer les paquets vers ou depuis un hôte, mais uniquement sur des ports spécifiques. Lorsqu'elle est sélectionnée, vous devez spécifier un ou plusieurs numéros de port TCP/IP. La description qui en découle correspond aux paquets destinés à ou envoyés vers au moins un des ports spécifiés. Par exemple, si vous avez spécifié les ports 99, 199, et 200, la description des paquets à mettre en correspondance produit le même effet que si vous exécutiez la commande suivante :

```
tcpdump -n -i eth0 "((port 99) or (port 199) or (port 200))"
```

Dans le fichier `ctc-conf.xml`, l'exemple ci-dessus correspondrait au langage XML suivant :

```
<ListenTos>
    <ListenTo>
        <Port>99</Port>
    </ListenTo>
    <ListenTo>
        <Port>199</Port>
    </ListenTo>
    <ListenTo>
        <Port>200</Port>
    </ListenTo>
</ListenTos>
```

Specific Host-Port Combinations
: Cette option permet de capturer ces paquets vers ou depuis des combinaisons hôte-port spécifiques. Lorsqu'elle est activée, vous pouvez spécifier l'hôte et les ports correspondants à capturer. La description qui en résulte correspond au moins à une des combinaisons où l'hôte source ou de destination correspond à l'hôte spécifié, et le port source ou de destination correspond au port spécifié.

Supposons que vous avez spécifié l'hôte et les combinaisons de ports suivants :

Hôte **Port**

127.0.0.1
80

172.16.0.1
1

172.16.0.2
2

La commande correspondante pour enregistrer le même trafic serait la commande unique suivante :

```
tcpdump -n -i eth0 "((host 127.0.0.1 and port 80) or \
(host 172.16.0.1 and port 1) or (host 172.16.0.2 and port 2))"
```

Dans le fichier `ctc-conf.xml`, l'exemple ci-dessus correspondrait au langage XML suivant :

```
<ListenTos>
    <ListenTo>
        <Address>127.0.0.1</Address>
        <Port>80</Port>
    </ListenTo>
    <ListenTo>
        <Address>172.16.0.1</Address>
        <Port>1</Port>
    </ListenTo>
    <ListenTo>
        <Address>172.16.0.2</Address>
        <Port>2</Port>
    </ListenTo>
</ListenTos>
```

Filtres VLAN

La PCA configure automatiquement ses filtres d'écoute afin d'autoriser la capture des paquets VLAN 802.1q sans configuration explicite.

Remarque : Exception : le trafic VLAN n'est pas capturé lorsque vous utilisez des filtres pour une plage de ports.

Si vous utilisez le package `tcpdump` pour l'analyse du trafic, vous devez appliquer manuellement les balises de filtre VLAN par le biais de la ligne de commande afin de voir les paquets VLAN. Dans la section précédente, la commande pour lancer `tcpdump` doit être étendue de la manière suivante afin d'activer la capture des paquets VLAN :

Remarque : supprimez les barres obliques à la fin de chaque ligne indiquant que la ligne continue.

```
tcpdump -n -i eth0 "((host 127.0.0.1 and port 80) or \
(host 172.16.0.1 and port 1) or (host 172.16.0.2 and port 2) or \
(vlan and host 127.0.0.1 and port 80) or \
(vlan and host 172.16.0.1 and port 1) or (vlan and host 172.16.0.2 and \
port 2))"
```

Console Web de la PCA - Onglet Distribution

L'onglet **Distribution** vous permet de définir les destinataires cible et les paramètres d'optimisation. Les captures d'écran suivantes affichent les options de configuration disponibles dans l'onglet **Distribution** de la console Web.

- Les interfaces réseau sont désormais affichées dans l'onglet **Utilitaires**. Voir «Console Web de la PCA - Onglet Utilitaires», à la page 163.

Destinataires cible

Cette liste indique les serveurs Tealeaf vers lesquels l'unité doit transférer les paquets de hits. Lorsque vous ajoutez un destinataire, une série d'écrans s'affiche pour configurer l'adresse et la sécurité de la distribution.

Target Recipients

Host or Address	Port	Security	Connection		Delete
TLI	1966	none	Ping	Speed	X
esta7296-b	1966	none	Ping	Speed	X
ms82hbr	1966	none	Ping	Speed	X

Add

Figure 22. Destinataires cible

Pour chaque homologue, les liens de la colonne Connexion (Ping et Vitesse) permettent de tester la connexion respectivement à l'aide d'une commande ping pour l'homologue ou d'un test de la vitesse de la connexion.

- Pour supprimer un homologue, cliquez sur l'icône **X** de la colonne Supprimer.



Figure 23. Ajouter un destinataire

Paramètre
Description

`Adresse de l'hôte`
Indique le nom d'hôte ou l'adresse IP du destinataire cible.

`Port de l'hôte`
Indique le numéro de port sur lequel le destinataire cible est en mode écoute.

`Activer la livraison sécurisée`
Détermine si la distribution sécurisée est activée ou non.

- Lorsque cette option est activée, vous devez importer un certificat SSL utilisable par la PCA. Voir «Création d'un certificat autosigné», à la page 207.

Nombre maximum de destinataires

Selon votre build de PCA, vous pouvez ajouter plus ou moins de destinataires.

- PCA Build 34xx et antérieure : `20`
- PCA Build 35xx et supérieure : `40`

Remarque : dans la mesure du possible, évitez d'utiliser un trop grand nombre de connexions homologues. Par défaut, la mémoire tampon de distribution de la file d'attente pour chaque homologue (`Max Queue Length`) est de 50 Mo. Selon le paramètre par défaut, pour activer 20 homologues, il est nécessaire de posséder 20 * 50 Mo = 1 Go de mémoire de processus pour les mémoires tampon de distribution. Si vous utilisez 40 homologues, 2 Go de mémoire de processus sont nécessaires, dépassant la limite de mémoire de processus 32 bits.

Si vous souhaitez utiliser autant d'homologues, réduisez à 25 Mo la mémoire de distribution de la file d'attente, en laissant à 1 Go l'utilisation totale de la mémoire de la file d'attente. Pour plus d'informations, voir le paramètre `Max Queue Length` de la section «Paramètres d'optimisation», à la page 94.

Exemple : ajouter un destinataire

Pour ajouter un destinataire, suivez les étapes ci-dessous :

1. Cliquez sur **Ajouter**. La page Ajouter un destinataire pour la distribution des hits s'ouvre.
2. Saisissez le domaine ou l'adresse IP du destinataire cible dans la zone **Adresse de l'hôte**.

   Remarque : si le système d'exploitation du serveur d'IBM Tealeaf Application de capture passive CX est configuré pour se connecter à un serveur DNS, vous pouvez saisir le nom de domaine. Dans le cas contraire, saisissez l'adresse IP. Tealeaf vous recommande d'utiliser une adresse IP statique afin d'éviter tout problème de DNS à l'avenir.
3. Dans la zone **Port d'hôte**, saisissez le port sur lequel le destinataire cible écoute les paquets de hits.
4. L'option Activer la distribution sécurisée permet de définir si la distribution sécurisée doit être utilisée ou non.
5. Pour utiliser cette option, cochez la case **Sécuriser** puis cliquez sur **OK**. La page Ajouter un certificat pour la distribution sécurisée s'ouvre. Sur cet écran, indiquez le certificat à utiliser lors de l'authentification du destinataire cible pour la distribution, en collant le certificat du destinataire dans la zone de texte Certificat du nouveau destinataire. Cliquez sur **OK**.
6. Si la distribution sécurisée est désactivée, ne cochez pas la case **Sécuriser** et cliquez sur **OK**.

Paramètres d'optimisation

Les paramètres d'optimisation vous permettent de définir les caractéristiques maximales de distribution.

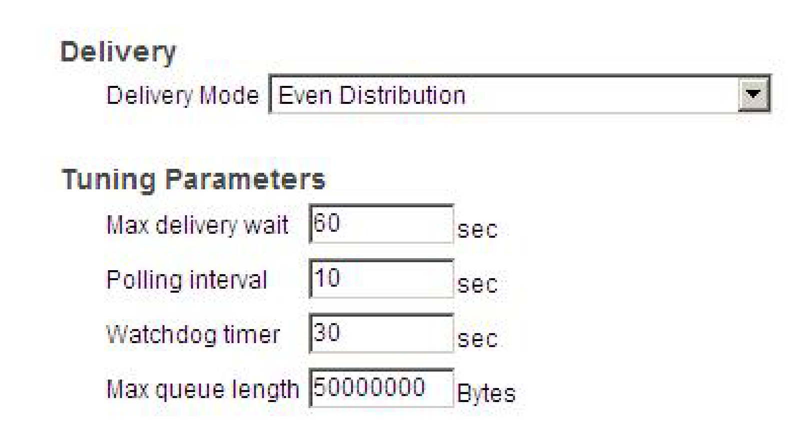


Figure 24. Paramètres d'optimisation (distribution)

Paramètre
Description

`Mode de livraison`
La fonction de mode de distribution permet à IBM Tealeaf Application de capture passive CX de distribuer le trafic par le biais de différentes méthodes à ses homologues de distribution (boîtes de dialogue des styles CSS). Il est possible de distribuer le trafic selon les méthodes suivantes :

- `Even Distribution` : le trafic est distribué de manière équilibrée entre les homologues. Par exemple, si quatre homologues sont configurés, chacun reçoit environ 25 % du trafic total.

  Remarque : dans PCA Build 3500 ou supérieure, lorsqu'un ou plusieurs homologues de distribution deviennent disponibles, le trafic est automatiquement redistribué entre les homologues actifs restants. Si un homologue inactif devient disponible, le trafic retourne à l'homologue et est rétabli pour assurer une distribution équilibrée. Cette méthode garantit une distribution équilibrée de la totalité du trafic sur tous les homologues de distribution actifs.
- `Failover` : cette méthode requiert deux homologues (principal et secondaire). L'homologue principal reçoit 100 % du trafic pendant que l'homologue secondaire est en veille. Si la connexion de l'homologue principal est perdue ou qu'un trop grand nombre de hits est abandonné, la PCA ferme la connexion à l'homologue principal et bascule vers l'homologue secondaire. Si la connexion à l'homologue secondaire échoue, la PCA tente de basculer à nouveau vers l'homologue principal. Si la PCA ne parvient pas à établir une connexion appropriée avec aucun des deux homologues, elle alterne jusqu'à ce qu'elle y parvienne.

  Remarque : il est probable que ce mode de distribution ne soit plus disponible dans la prochaine édition.
- `Clone` : cette option correspondait au comportement par défaut dans la version précédente. Chaque homologue obtient la totalité du trafic.
- `None` : cette option remplace l'option "deliver to null". Si elle est sélectionnée, le trafic est abandonné avant d'être envoyé vers les homologues de distribution qui constituent uniquement une aide au débogage.

`Attente maximale de livraison`
Permet de définir la durée du minuteur utilisé pour envoyer des paquets de hits. Lorsque le minuteur expire, l'unité tente d'envoyer tous les paquets de hits aux destinataires cible.

`Intervalle d'interrogation`
Ce paramètre n'est pas utilisé actuellement.

`Horloge de surveillance`
Indique le temps maximal (en secondes) durant lequel établir une connexion au serveur IBM Tealeaf CX. Si le délai est dépassé, la connexion est marquée comme déconnectée. La valeur par défaut est de `30` secondes.

`Longueur maximale de la file d'attente`
Permet de définir la taille maximale de la file d'attente de distribution. Si la file d'attente atteint cette limite, le système annule les nouveaux paquets de hits jusqu'à ce que la file raccourcisse. Ainsi, le système empêche le retard de causer une panne.

Utilisation du service de transport Tealeaf comme horloge de référence

Cette section contient les informations nécessaires à la configuration d'un hôte exécutant le service de transport Tealeaf en tant qu'horloge de référence. Lorsqu'il est activé, le service de transport Tealeaf défini est contacté toutes les 15 minutes afin d'indiquer l'heure. L'horloge système dérive en fonction de celle du service de transport. La dérivation signifie que l'heure locale du logiciel Passive Capture n'est en fait pas fixée sur l'heure exacte de la machine distante du service de transport.

Si l'heure locale est inférieure à l'horloge distante, l'horloge système gagne du temps petit à petit. Si l'heure locale est plus avancée que l'heure distante, l'horloge système ralentit afin de correspondre au mieux à l'heure distante.

Use TeaLeaf Transport Service as Time Source

Unless you are synchronizating time using another mechanism, such as NTP, you normally want to use one of the delivery peers as a time source.

Host or Address | css | [Specifying a time source host will enable time synchronization.]

Port | 1966 | [Optional: The default value is 1966.]

Figure 25. Utilisation du service de transport Tealeaf comme horloge de référence

Paramètre
Description

Hôte ou adresse
Désigne le nom de domaine ou l'adresse IP de l'hôte qui exécute le service de transport Tealeaf à utiliser comme horloge de référence. Si vous ne souhaitez pas vous synchroniser avec une horloge de référence, ne renseignez pas cette zone.

Port
Désigne le port sur lequel l'hôte de l'horloge de référence écoute les requêtes concernant l'heure. Si vous ne souhaitez pas vous synchroniser avec une horloge de référence, ne renseignez pas cette zone.

Distribution de statistiques au service de transport Tealeaf

Cette section contient des informations sur la configuration des hits de statistiques. Pour ces hits, vous pouvez contrôler les cinq paramètres suivants :

Deliver Statistics to TeaLeaf Transport Service

You normally send statistics hits to the same delivery peer that receives the captured hits for your site and the SessionRouter on the receiving end will send the statistics hit to the correct downstream component.

Enabled ☑

Host or Address | css

Interval (seconds) | 60

Port | 1966

Use SSL ☑

Figure 26. Distribution de statistiques au service de transport Tealeaf

Paramètre
Description

Activé
Si cette case est cochée, les hits de statistiques sont activés. Dans le cas contraire, la fonction est désactivée.

Hôte ou adresse
Cette zone contient le nom d'hôte ou l'adresse IP de la machine qui exécute le service de transport Tealeaf devant recevoir les hits de statistiques.

Intervalle
: Cette valeur, un nombre positif, représente le laps de temps minimum en secondes entre les tentatives d'envoi des hits de statistiques. Si vous indiquez zéro, les hits de statistiques ne seront pas envoyés.

Port
: Saisissez le numéro de port TCP/IP à utiliser lors de votre connexion au service de transport Tealeaf sur l'hôte.

Utiliser SSL
: Indique si la connexion au service de transport Tealeaf doit utiliser le protocole SSL.

Console Web de la PCA - Onglet Clés SSL

Cet onglet vous permet de consulter et de modifier la liste des clés chargées et celle des clés manquantes. Pour passer d'une liste à l'autre, utilisez le bouton d'option correspondant :

- La vue Clés privées chargées vous permet d'ajouter, de modifier et de supprimer des clés privées pour des serveurs sécurisés.
- La vue Clés privées manquantes vous permet d'afficher les informations sur ces clés, de les ignorer ou de les effacer.
- Vous pouvez également charger des certificats SSL dans plusieurs formats. Voir «Clés de capture», à la page 101.

Clés chargées

Dans l'onglet **Clés SSL**, vous pouvez consulter les clés privées chargées et les clés privées manquantes.

- A partir de PCA Build 3500, les clés chargées peuvent être affichées au format IPv6. Voir «Comment la PCA gère-t-elle la capture des adresses IPv6 ?», à la page 289.

Help | Guide

Capture Keys - Automatically loaded keys

Select private keys to view: Loaded Missing

The following keys are configured to be loaded when capture starts.

Select one entry to edit, or multiple entries to delete.

	Label	File	Date
☐	tealeaf-tts	/usr/local/ctccap/etc/tealeaf-tts.pem	Feb 24 2009 11:19:48 AM
☐	cztest	/usr/local/ctccap/etc/cztest.pem	Feb 17 2009 09:57:13 PM

Edit Delete

Add a private key:

Label: File: Add

Save Changes Revert to Saved

Figure 27. Onglet Clés SSL - Vue Clés chargées

- Pour plus d'informations sur la vue Clés manquantes, voir «Clés manquantes», à la page 99.

Colonne
: **Description**

case à cocher
: Cochez la case pour sélectionner un certificat.

`Libellé`
: Représente le libellé du certificat.
  - Pour plus d'informations sur la modification du libellé, voir «Modification d'une clé privée», à la page 99.

`Fichier`
: Indique le chemin et le nom du fichier `.pem`.
  - Pour plus d'informations sur la modification du nom du fichier écran, voir «Modification d'une clé privée», à la page 99.

`Date`
: Indique l'horodatage de la première occurrence lorsque la PCA a rencontré un paquet en utilisant la clé.

- Pour plus d'informations sur le chargement d'une clé privée, voir «Ajout d'une clé privée», à la page 99.
- Pour modifier une clé chargée, cochez la case en regard de cette dernière, puis cliquez sur **Modifier**. Voir «Modification d'une clé privée», à la page 99.
- Pour supprimer une clé chargée, cochez la case en regard de cette dernière, puis cliquez sur **Supprimer**.
- Pour enregistrer vos modifications, cliquez sur **Enregistrer les modifications**.

- Pour annuler les modifications non enregistrées et rétablir celles qui l'ont été, cliquez sur **Rétablir version enregistrée**. Le jeu de clés précédemment enregistré est rechargé.

Modification d'une clé privée

Vous pouvez modifier une clé privée pour charger une clé, lui attribuer un libellé plus significatif et indiquer le chemin complet du fichier de clés.

- Pour enregistrer les modifications cliquez sur **OK**.

Ajout d'une clé privée

Add a private key:

Label: File: Add

Figure 28. Ajouter une clé privée. Pour ajouter une clé privée, procédez comme suit :

Remarque : seules les clés privées (`.pem` et `.pfx`) converties au format **`.ptl`** sont prises en charge.

1. Sélectionnez le bouton d'option **Chargé**.
2. Saisissez le nom de domaine ou l'adresse IP du destinataire dans la zone **Libellé**. La valeur saisie désigne le libellé utilisé pour identifier la clé d'affichage.
3. Dans la zone **Fichier**, saisissez le nom du fichier contenant la clé privée dont doit se servir l'unité pour décoder les sessions SSL. Cette zone doit contenir un nom de fichier absolu et complet.
4. Cliquez sur **Ajouter**.
5. Cliquez sur **Enregistrer les modifications** au bas de la page.
6. Vous pouvez à présent modifier, afficher ou supprimer la clé en cliquant sur les boutons correspondants.

Clés manquantes

Pour voir et modifier la liste des clés privées manquantes, cliquez sur le bouton d'option **Manquantes** en haut de l'onglet Clés SSL.

- A partir de PCA Build 3500, les clés manquantes peuvent être affichées au format IPv6. Voir «Comment la PCA gère-t-elle la capture des adresses IPv6 ?», à la page 289.

Help | Guide

Capture Keys - Automatically loaded keys

Select private keys to view: Loaded Missing

Click on a host/port entry to view certificate information.

Host : Port	Date
65.55.13.91:443	Jan 24 2011 03:24:15 AM
65.54.51.253:443	Jan 25 2011 03:28:49 PM
63.194.158.210:443	Jan 27 2011 04:32:17 PM
65.55.25.60:443	Jan 24 2011 10:43:56 AM
207.46.21.124:443	Jan 24 2011 02:55:28 AM
207.46.21.123:443	Jan 19 2011 09:02:12 PM
65.55.27.219:443	Jan 22 2011 02:19:30 PM
65.55.184.156:443	Oct 28 2009 02:28:26 PM
65.55.200.156:443	Jan 25 2011 04:46:40 AM
65.55.200.155:443	Jan 26 2011 03:50:29 PM
65.55.27.220:443	Jan 23 2011 09:06:11 AM
65.55.185.28:443	Oct 23 2009 03:11:49 PM
65.55.184.155:443	Jan 18 2011 12:16:19 PM
65.55.184.26:443	Jan 24 2011 10:16:23 PM
65.55.184.27:443	Jan 20 2011 01:15:39 PM

Select All   Clear Selected   Ignore Selected

Use Clear Selected to remove one or more missing key entries from the list.
Use Ignore Selected to add the IP/Port combination to the list of ignored traffic.

Save Changes

Figure 29. Onglet Clés SSL - Vue Clés manquantes

Colonne
Description

case à cocher
Cochez la case pour sélectionner une clé.

Hôte:Port
Indique l'adresse IP de l'hôte et le numéro de port du certificat SSL.

Date
Indique l'horodatage de la première occurrence depuis le dernier redémarrage de la PCA lorsqu'un paquet SSL dont il manquait une clé unique SSL a été détecté.

- La zone **Date** des paquets SSL suivants pour lesquels la même clé est manquante n'est pas mise à jour.

- Pour effacer la date, cochez la case et cliquez sur **Supprimer la sélection**. L'horodatage est mis à jour lorsque l'instance de paquets suivante, dont la clé SSL manquante a été supprimée, est détectée.

Pour sélectionner une clé SSL, cochez la case à côté de l'hôte et du port du certificat.

- Pour sélectionner tous les certificats manquants, cliquez sur **Sélectionner tout**.
- Pour ignorer les certificats sélectionnés, sélectionnez **Ignorer la sélection**.
- Pour supprimer les certificats sélectionnés, sélectionnez **Supprimer la sélection**.
- Pour enregistrer les modifications, cliquez sur **Enregistrer les modifications**.

Clés de capture

A partir de l'onglet **Clés SSL**, vous pouvez charger des certificats SSL au format de texte en clair `.pem` ou au format `.pfx` protégé par mot de passe, à convertir en `.ptl` pour les utiliser dans la PCA.

- Voir «Paramétrage des clés SSL chiffrées», à la page 193.

Si vous avez accès au logiciel PCA sur le serveur Linux, vous pouvez déplacer les certificats SSL dans un répertoire défini pour la conversion automatique au format `.ptl`.

- Voir «Exportation la clé privée SSL», à la page 198.
- Voir «Exportation la clé privée SSL», à la page 198.

Génération de vos propres certificats SSL

Voir «Création d'un certificat autosigné», à la page 207.

Console Web de la PCA - Onglet Pipeline

L'onglet Pipeline permet aux utilisateurs de modifier les paramètres de configuration comme la capture, les limites et les ID de cookie.

- Si les zones ne sont pas renseignées, le périphérique tente de lire les valeurs par défaut du fichier `ctc-conf-defaults.xml`.

Vous pouvez sélectionner une des deux vues pour afficher les paramètres du pipeline :

- Paramètres du pipeline : permet de définir la mise en sessions des données, les niveaux de temps, le mode de capture et plus encore. Voir «Paramètres du pipeline», à la page 102.
- Modifier la liste des types : permet de définir les types de données et les extensions de fichier à inclure ou à exclure de la capture. Voir «Listes des types de capture», à la page 112.

  Remarque : vous devez consulter les types de capture de la PCA lors de l'installation d'IBM Tealeaf Application de capture passive CX ou si l'application Web contrôlée est mise à jour. Voir «Listes des types de capture», à la page 112.

Paramètres du pipeline

Pipeline Instances

Instances: 1 (default=1)

Queue2 Size: 100 (default=100)

Data Sessioning

Use Sessioning

Ignore Case

Field Name:

Field Section:

Field Offsets:

X-Forwarding

Enable

Field Name:

Session Sampling

[Session sampling requires data sessioning to be enabled.]

Use Session Sampling

Sampling: 100%

Capture Mode:

Business

BusinessIT

Capture Request Methods:

GET

POST

PUT

Time Grading

Use Time Grading

Web Server Page Gen

Network Transit

Round Trip

Grade	Description	Max Value	
0	ExcellentWS	200000	µs (~0.2s)
1	NormalWS	1000000	µs (~1s)
2	HighNormalW	2000000	µs (~2s)
3	HighWS	4000000	µs (~4s)
4		(Anything higher)	

Hit Processing

Include raw request

Include response headers

Decode URL fields

Cookie parser

Enable UnReqCancelled

Inflate compressed response

Preserve responses when inflate fails

Deflate hits sent to target recipients

Enable I18N (CX Release 7.0 or later required)

Delete Images on PCA side

Enable TLI

Max response size (bytes): 1572864

Default response encoding: None

Default request encoding: None

Figure 30. Paramètres du pipeline

Instances du pipeline

Par défaut, la PCA est configurée pour créer une instance unique du processus pipelined à utiliser pour toutes les instances de l'application Passive Capture. Si

nécessaire, il est possible de créer des instances du processus pipelined supplémentaires afin de distribuer plus efficacement le travail dans les ressources disponibles.

Remarque : plusieurs instances du pipeline de la PCA sont disponibles dans PCA Build 3403 ou supérieure.

Lorsque plusieurs instances du processus pipelined sont créées, chaque instance de la PCA soumet les paquets TCP. Ces derniers sont assemblés par le processus reassd dans la file d'attente du pipeline. Celle-ci distribue ensuite, de façon circulaire, les paquets aux instances pipelined configurées pour qu'ils soient traités.

- Le processus pipelined de la PCA traite individuellement les hits HTTP, par exemple il en supprime, applique des règles de confidentialité, compresse les données, etc. Voir Chapitre 1, «Présentation de Passive Capture», à la page 1.

L'efficacité de l'utilisation de plusieurs pipelines dépend du nombre de coeurs de processeur disponibles. La règle empirique générale est d'allouer un coeur de processeur disponible à chaque instance de pipeline. Si quatre coeurs de processeur sont disponibles, vous ne devez pas configurer plus de quatre instances de pipeline pour une charge complète du processeur.

Remarque : vous devez toujours consacrer au moins un coeur de processeur de la machine aux processus système.

- En théorie, la limite maximale pour le nombre de pipelines est de `128`. Il est peu probable que vous atteigniez cette limite.

Remarque : tous les pipelines agissent selon le même ensemble de règles de configuration. Il ne doit y avoir aucune différence entre les règles de confidentialité ou toute autre option de configuration des pipelines.

Paramètre
: **Description**

`Instances`
: Indique le nombre d'instances du processus pipelined.

  - Pour définir un autre nombre d'instances, saisissez une valeur dans la zone de texte et cliquez sur **Enregistrer les modifications**.

    Remarque : référez-vous aux valeurs précédentes lorsque vous créez de nouvelles instances du processus pipelined. Ajoutez d'abord une instance puis vérifiez le résultat et l'impact sur les ressources disponibles du serveur de la PCA.

`Queue2 Size`
: Indique la taille (en mégaoctets) de la file d'attente qui approvisionne les instances du processus pipelined. Par défaut, cette valeur est de `100`.

Pour récupérer les statistiques d'une instance de pipeline individuelle, exécutez les commandes suivantes.

Statistiques de l'instance 0 :

```
ctcstats instdata
```

Statistiques de l'instance #N

```
ctcstats -I<#N> instdata
```

où

- <#N> représente l'identificateur de l'instance.

Mise en sessions des données

Il est possible de configurer la PCA afin de créer un ID session pour chaque hit basé sur les cookies injectés dans la requête. Lorsque cette fonction est activée, vous pouvez configurer la section de la requête et les informations de zone contenant l'ID session.

- Le cookie utilisé pour ouvrir une session doit être unique et conservé pour chaque hit d'une session.

Lorsque l'option de mise en sessions des données est activée, l'ID ou le cookie de session défini par la valeur de la zone `Field Name` est haché pour créer l'ID session Tealeaf (`TLTSID`). Tealeaf Cookie Injector créer cette valeur lorsqu'il est en cours d'utilisation.

Remarque : si vous utilisez Tealeaf Cookie Injector, n'activez pas cette fonction. Il fournit des identificateurs uniques garantis pour les données de session capturées par Tealeaf. Voir section "Installation et configuration de Tealeaf Cookie Injector" du *Manuel d'IBM Tealeaf Cookie Injector*.
S'il n'y a aucun cookie de session, vous pouvez interrompre la session pour d'autres données de hit en déployant l'agent de session de mise en sessions du pipeline de Windows sur le serveur de traitement. Voir section "Agent de session de mise en sessions" du *Manuel de configuration d'IBM Tealeaf CX*.

Propriété
Description

`Nom de zone`
Indique le nom du cookie avec lequel vous souhaitez effectuer une mise en sessions. Les valeurs acceptées sont `jsessionid` et `aspsessionid`.

- Pour mettre en session plusieurs cookies, vous pouvez insérer plusieurs valeurs dans cette zone en les délimitant. Les délimiteurs acceptés sont la virgule (**,**) et le point-virgule (**;**).

`Field Section`
Vous pouvez utiliser cette zone pour spécifier la section de la requête dans laquelle rechercher le contenu de la zone `Field Name`. Si cette valeur n'est pas spécifiée, la zone est recherchée dans la totalité de la requête et la première occurrence est utilisée.

`Field Offsets`
Vous devez mettre en session une partie spécifique du cookie de session comme le spécifie la zone `Field Name`. Par exemple, lorsque la valeur de votre cookie a une longueur de 32 caractères, si vous définissez la valeur à `0 15`, les 16 premiers caractères seront mis en session.
Cette fonction est utile lorsque le cookie de session est complété par une chaîne statique :

```
. jsessionid=<unique keystuff here>mycookie;
```

X-Forwarding

X-forwarding, une norme standard, permet de suivre l'adresse IP d'origine d'un client se connectant à un serveur parmi plusieurs serveurs, comme des serveurs proxy ou des équilibreurs de charge.

- Lorsque cette fonction est activée, il est possible de renseigner la zone `HTTP_X_FORWARDING` avec les adresses IP de chaque serveur qui consulte et transfère la demande.

- Lorsque le contenu est renvoyé par le serveur Web d'origine, il est transmis à chaque serveur répertorié dans la zone HTTP_X_FORWARDING. Chaque serveur en supprime la référence dans la zone et le transfère au prochain serveur de la chaîne.
- Ainsi, le contenu peut passer par plusieurs serveurs entre le client auteur de la demande et le serveur fournisseur d'origine.
- L'utilisation des numéros de port dans les adresses IP (par exemple <ip_address>:XXXX) n'est pas prise en charge.

  Remarque : cette fonction est disponible dans PCA Build 3501 ou supérieure.
- Si un en-tête CLIENT_IP est disponible, il est préférable de l'utiliser pour la source X-Forwarding, dans la mesure où il contient généralement une seule adresse IP.

En fonction de la configuration de votre application Web, vous pouvez définir, à partir de la PCA, la zone d'en-tête utilisée pour spécifier la zone HTTP_X_FORWARDING. Cette zone renvoie à la zone source de l'adresse IP au format IPv4 ou IPv6.

Remarque : même si ce n'est pas obligatoire, il est possible d'utiliser la fonction X-forwarding afin de gérer le transfert pour les adresses au format IPv4 et IPv6.

A partir de PCA Build 3501, vous pouvez configurer la source de l'adresse REMOTE_ADDR insérée dans la PCA.
1. Pour activer X-forwarding, cochez la case **Activer**.
2. Saisissez le nom de la valeur de la zone du nom de variable de l'en-tête de la demande HTTP contenant l'adresse IP X-Forwarding.
   - Dans les builds 3501 et 3502 de la PCA, vous devez insérer le nom réel formaté de l'en-tête HTTP. Cependant, il est difficile de se le procurer. Les valeurs insérées dans la section [env] de la demande ne fonctionnent pas.
   - A partir de PCA Build 3600, vous pouvez utiliser les traits de soulignement, les tirets et le préfixe HTTP_ dans l'entrée de la valeur de zone ainsi que les entrées prises en charge dans les builds 3501 et 3502. Par exemple, pour la valeur de zone X-FORWARDED-FOR, les variantes suivantes sont acceptées :
     ```
     HTTP_X_FORWARDED_FOR
     X_FORWARDED_FOR
     X-FORWARDED-FOR
     ```

     Remarque : le nom de zone est sensible à la casse.

     Remarque : la zone source X-forwarding peut contenir plusieurs adresses IP, chacune devant être séparée par une virgule. Les points-virgules ou tout autre délimiteur de zone ne sont pas pris en charge. Dans une ligne à entrées multiples, la première adresse est utilisée si elle est correctement délimitée. Dans le cas contraire, la ligne entière est utilisée et n'est pas correctement traitée.
3. Cliquez sur **Enregistrer les modifications**.

Lorsque l'option X-forwarding est activée par le biais de l'onglet Pipeline, la zone d'en-tête spécifiée est analysée afin d'identifier le nom de la zone de demande à utiliser pour REMOTE_ADDR. Cette zone est ensuite analysée afin de reconnaître la valeur à insérer dans REMOTE_ADDR.
- La recherche est sensible à la casse.

- La zone identifiée est analysée pour détecter le formatage correct. Si aucune valeur correspondante n'est trouvée, aucune action n'est prise et REMOTE_ADDR est normalement renseigné.

  Remarque : Dans les builds antérieures à PCA Build 3501, l'identification de HTTP_X_FORWARDING était gérée par les règles de confidentialité dans le pipeline de la PCA. Avant de déployer cette nouvelle méthode, exécutée avant que le contenu ne soit envoyé dans le pipeline de la PCA, assurez-vous que les règles de confidentialité de la PCA pour la gestion de HTTP_X_FORWARDING sont désactivées. Voir «Téléchargement de la configuration de confidentialité», à la page 118.

Si une correspondance est trouvée, la valeur est insérée dans REMOTE_ADDR, et la valeur précédente est insérée dans la variable de demande REMOTE_ADDR_ORIG.

Exemple (IPv4)

```
REMOTE_ADDR=10.20.30.40
IPV6_REMOTE_ADDR=0000:0000:0000:0000:0000:FFFF:0A14:1E28
REMOTE_ADDR_ORIG=10.10.28.82
```

Exemple (IPv6)

```
REMOTE_ADDR=abcd::100:B200:CD10:10
IPV6_REMOTE_ADDR=ABCD:0000:0000:0000:0100:B200:CD10:0010
REMOTE_ADDR_ORIG=10.10.28.82
```

A partir de la version 8.4, les valeurs détectées dans REMOTE_ADDR après X-forwarding sont converties au format IPv6 et insérées dans la variable IPV6_REMOTE_ADDR. Ces valeurs sont indexées pour la recherche. Voir «Comment la PCA gère-t-elle la capture des adresses IPv6 ?», à la page 289.

Echantillonnage de session

Lorsqu'il est activé, l'échantillonnage de session définit un pourcentage de sessions à transférer vers l'homologue de distribution. Les sessions restantes sont supprimées de la capture. L'échantillonnage de session permet de capturer d'importants volumes de données sans surcharger le système avec des volumes de production.

Remarque : cette fonction supprime les données de session du flux de capture et constitue une fonction de débogage. Nous vous conseillons de ne pas l'activer.

Mode de capture

Le paramètre Mode de capture définit les types de données devant être capturées et déplacées par la PCA à partir du flux de capture. Les paramètres suivants sont disponibles :

Mode de capture
  Description

Business
  Configure le logiciel Passive Capture afin de capturer uniquement les demandes HTTP(S) et les objets réponse pour les demandes de pages .business. (par exemple, HTML, ASP, JSP). Les objets statiques comme les feuilles de style, JavaScript et les fichiers image ne sont pas capturés par la PCA.

  - Les clients de relecture Tealeaf peuvent acquérir et charger ces éléments selon les besoins lors de la réexécution.

Remarque : Le mode de capture Business est le paramètre par défaut. Tealeaf recommande l'utilisation de ce mode.

BusinessIT
Configure Passive Capture afin de capturer les demandes et les réponses HTTP(S) ainsi que les objets de fichier associés à chaque hit. Ces objets statiques, comme les fichiers image, sont capturés par la PCA et transférés vers le pipeline de Windows où ils sont évalués de manière approfondie.

Remarque : En mode BusinessIT, le corps du contenu de l'objet réponse n'est pas enregistré. Seuls le fichier image et la demande sont capturés puis traités.

Remarque : lorsque vous passez du mode de capture Business à BusinessIT, le volume du trafic capturé, traité et stocké par Tealeaf augmente considérablement. Avant de changer de mode, consultez la totalité de votre solution Tealeaf afin de vous assurer que vous possédez les ressources système pour gérer l'augmentation du contenu. Pour plus d'informations, veuillez contacter les services professionnels de Tealeaf.

Méthodes de demande de capture

Indique les méthodes HTTP à inclure. Les méthodes GET, POST, et PUT sont prises en charge.

Remarque : Les demandes de type HEAD ne sont pas prises en charge pour la capture.

Niveau de temps

Lorsqu'il est activé, ce paramètre permet d'attribuer un niveau à un hit pour l'une des caractéristiques suivantes :

Caractéristique
Description

`Web Server Page Gen`
Correspond au temps que met le serveur Web pour charger la page.

`Network Transit`
Mesure la vitesse du réseau en fonction du temps qu'a passé un paquet sur le réseau.

`Round Trip`
Correspond au temps de déplacement d'un paquet du client vers le serveur Web.

En fonction de ces trois critères, le paramètre Niveau de temps attribue au hit une valeur numérique. Il est possible de modifier la description des niveaux par défaut (Excellent, Normal, NormalElevé, Elevé) ainsi que leurs valeurs maximales correspondantes.

Traitement des hits

Paramètre
Description

`Include Raw Request`
Détermine si RawRequest est actif. RawRequest constitue une aide au

débogage. La valeur par défaut est `False` (désactivé). Lorsque ce paramètre est activé (`True`), les en-têtes de demande HTTP sont ajoutés au hit.

Remarque : Tealeaf vous recommande fortement de définir la valeur sur `False`. Dans le cas contraire, les données sont ajoutées à chaque hit.

`Include Response Headers`
Détermine si les en-têtes de réponse sont actifs. Ils constituent une aide au débogage. La valeur par défaut est `False` (désactivé). Lorsque ce paramètre est activé (`True`), les en-têtes de réponse HTTP (au format Tealeaf et pas nécessairement la représentation HTTP exacte) sont ajoutés au hit.

Remarque : Tealeaf vous recommande fortement de laisser la valeur `False`. Dans le cas contraire, les données sont ajoutées à chaque hit.

`Decode URL fields`
Cette option définit si les adresses des zones URL doivent être décodées.

`Cookie Parser`
Lorsque cette option est sélectionnée, une section de cookies est ajoutée à la demande.

`Enable UnReq Cancelled`
Lorsqu'elle est activée, cette option vérifie les 100 derniers octets du corps de réponse pour `</html` quand `capturetype=1` et est marquée comme annulée.

`Inflate compressed response`
Lorsque cette option est sélectionnée, les réponses sont automatiquement décompressées dans le pipeline de la PCA. Si une réponse possède un en-tête de codage de contenu dont la valeur est `deflate`, `gzip`, ou `x-gzip`, son corps est alors susceptible d'être décompressé à partir de son état compressé. Lorsque cette option est sélectionnée, une tentative de décompression de la réponse est effectuée.

Remarque : ce paramètre doit être défini sur `false`. Si vous activez cette option, le volume des données transmises entre le serveur IBM Tealeaf Application de capture passive CX et le service de transport peut augmenter considérablement.

- Lorsque la décompression échoue, un message est consigné dans le journal `notice`.
- Lorsque la décompression a fonctionné, la valeur de l'en-tête de codage de contenu est écrasée par le caractère `X`, par exemple Codage de contenu : `XXXX`.
- Dans PCA Build 3502 ou supérieure, les POST compressés sont automatiquement décompressés pour les types de codage de contenu, peu importe le type de contenu, pour prendre en charge la capture des données à partir des environnements de capture des clients Tealeaf.
  - Dans PCA Build 3501 ou antérieure, il s'agissait de l'option `Inflate compressed requests and responses`.

`Preserve responses when inflate fails`
Lorsqu'une réponse de hit est décompressée et que le processus de décompression échoue, la réponse est remplacée par un code HTML signalant une erreur de décompression. Sélectionnez cette option pour désactiver le remplacement avec le code HTML, cela préservera la réponse d'origine.

Deflate hits sent to target recipients
: Sélectionnez cette option pour les réponses de hit décompressées avant d'être envoyées à un destinataire cible. Les réponses de hit sont compressées à l'aide de la méthode deflate HTTP. Activez cette option afin de réduire l'utilisation de la bande passante du réseau pour distribuer les hits de Tealeaf au service de transport Tealeaf.

Enable I18N
: Lorsque cette option est sélectionnée, la prise en charge de l'internationalisation est activée dans la PCA. Les zones d'URL de la demande sont codées en UTF-8 et une tentative de détection du codage du corps de réponse est effectuée. Voir section "Prise en charge de l'internationalisation" du *Manuel d'installation d'IBM Tealeaf CX*.

  Remarque : il existe un problème de codage des caractères des données JSON provenant d'un environnement de capture d'un client Tealeaf. Voir «Solution de contournement des caractères JSON codés», à la page 111.

  Remarque : il est possible d'activer ce paramètre uniquement dans les PCA connectées à IBM Tealeaf CX Version 7.0 ou supérieure.

Delete Images on PCA side
: Lorsqu'elle est activée, cette option supprime du flux de capture les hits d'image répondant à des critères spécifiques. Voir «Suppression des images dans la PCA», à la page 110.

Enable TLI
: Si vous déployez un serveur TLI dans votre environnement Tealeaf, vous pouvez activer la capture du contenu d'image afin de le stocker en aval sur le serveur TLI. Voir «Activation de la capture d'image pour un serveur TLI», à la page 111.

Taille maximale de réponse
: Taille maximale autorisée pour la réponse (en octets). La valeur par défaut est fixée à `1572864` (1,5 Mo).

Default Response Encoding
: Cette valeur est utilisée lorsque la PCA n'est pas en mesure de détecter le type de codage d'une réponse.

  Remarque : Les informations ci-après ne s'appliquent qu'à IBM Tealeaf version 9.0A.

  CX PCA version 3700 contient les sélections supplémentaires pour la prise en charge améliorée des caractères de support international (EICS) à partir de ce qui est disponible dans CX PCA version 3650.

Default Request Encoding
: Cette valeur est utilisée lorsque la PCA n'est pas en mesure de détecter le type de codage d'une demande.

  Remarque : Les informations ci-après ne s'appliquent qu'à IBM Tealeaf version 9.0A.

  CX PCA version 3700 contient les sélections supplémentaires pour la prise en charge améliorée des caractères de support international (EICS) à partir de ce qui est disponible dans CX PCA version 3650.

Remarque : Les informations ci-après ne s'appliquent qu'à CX PCA génération 3700.

Nombre total abandonné en raison des erreurs d'encodage ICU
Cette statistique signale chaque occurrence où un hit (demande ou réponse) ne peut pas être encodé en UTF-8, ce qui entraîne l'abandon du hit complet. Ce scénario génère également une erreur (ERR) dans le journal.

Suppression des images dans la PCA

Dans les builds antérieures à PCA Build 3502, l'application utilisait des options de configuration et une logique intégrée afin de gérer la suppression automatique des images des hits capturés, réduisant considérablement l'espace nécessaire pour le stockage des sessions. Lorsque le mode de capture BusinessIT a été créé pour la PCA, certains types de contenu d'images pouvaient être capturés et transférés vers le pipeline de Windows où ils étaient supprimés à l'aide de l'agent de session DelImages.

- Pour plus d'informations sur le mode BusinessIT, voir «Mode de capture», à la page 106.
- Pour plus d'informations sur la fonction DelImages pour le pipeline de Windows, voir "Agent de session de suppression des données" du *Manuel de configuration d'IBM Tealeaf CX*.

A partir de PCA Build 3502, la fonctionnalité DelImages est désormais disponible dans le pipeline de la PCA. Lorsque DelImages est activé dans la PCA, le volume des données capturées, traitées et transférées sur le serveur Windows est réduit.

Remarque : pour assurer la capture du contenu d'image dans votre environnement Tealeaf, appliquez ce paramètre à partir des onglets Pipeline de toutes les instances de la PCA.

Lorsqu'un hit remplit les critères suivants, il est identifié comme un hit image puis supprimé :

- `Delete Images on PCA side` est activé.
- L'extension de fichier pour la réponse est répertoriée dans la liste des extensions de fichier exclues. Voir «Extensions de fichier exclues», à la page 116.
- Ou encore lorsque l'un des critères suivants est rempli :
  1. PCA `CaptureType=3` et (`StatusCode = 200` ou `StatusCode = 304`)
     – Ce critère détermine si la PCA se trouve en mode BusinessIT (CaptureType=3), une demande d'image est renvoyée avec le statut "okay" ou "inchangé" (StatusCode =304).
  2. `HTTP_USER_AGENT contient "RealiTeaViewer"` ou `HTTP_USER_AGENT contient "TeaLeafFileGetter"`
     – Ce critère détermine si la demande est effectuée par l'application de bureau de Tealeaf IBM Tealeaf Visualiseur CX RealiTea pour le contenu d'image du serveur d'origine lors de la réexécution. Ces demandes ne doivent pas être capturées.

Si les critères précédents sont remplis, le hit d'image est abandonné.

- Lorsque cette fonction est activée, si `CaptureType=1` et que le type de contenu de la réponse est répertorié dans la liste Inclure l'extension, la demande et la réponse sont capturées.

Dans l'onglet Statistiques, le nombre total de hits d'image s'affiche dans l'indicateur `Total dropped due to businessIT mode and DelImages feature set`. Voir «Statistiques par instance», à la page 137.

Solution de contournement des caractères JSON codés

Dans certains cas, il est possible que les caractères spéciaux soumis sous forme de données au format JSON (UTF-8) par l'un des environnements de capture côté client Tealeaf soient codés lors du traitement effectué par Tealeaf. A partir de la PCA, vous pouvez configurer des paramètres pour vous assurer que ces caractères sont correctement consommés.

Si vous avez activé la conversion I18N dans l'onglet **Pipeline**, suivez les étapes ci-dessous.

1. Dans l'onglet **Pipeline** de la console Web de la PCA, définissez `Default request encoding` sur `UTF-8`. Les zones URL de demande sont définies selon l'encodage UTF-8. La PCA utilise le codage UTF-8 lorsqu'elle n'est pas en mesure de détecter un type de codage.

   Remarque : cette modification, pour indiquer que les zones URL de demande sont codées en UTF-8, peut causer des problèmes de conversion lorsque les zones ne sont pas codées en ISO 8859 ou en UTF-8.
2. Cliquez sur **Enregistrer les modifications**.

En fonction des modifications de la configuration précédentes, les données au format JSON soumises en UTF-8 ne sont pas converties à un codage différent. Si vous définissez le codage UTF-8 par défaut, les données ne seront pas converties dans la mesure où les données JSON sont soumises dans la section `[RequestBody]`, contenue dans la section `[urlfield]`. Par conséquent, les données sont correctement représentées dans Tealeaf.

Activation de la capture d'image pour un serveur TLI

Dans Tealeaf, il est possible de déployer un serveur TLI pour capturer du contenu statique comme des images, du contenu JavaScript et des feuilles de style, dans des archives permanentes. Lors de la réexécution, les demandes de ce contenu statique font référence aux archives statiques permettant d'éviter les demandes inutiles ou interdites auprès du serveur d'origine. Un serveur TLI vous permet de conserver une copie du contenu statique de chaque session retraçant l'expérience du visiteur à des fins de réexécution et de contrôle.

- Pour plus d'informations sur les serveurs TLI, voir section "Gestion des archives statiques" du *Manuel d'administration d'IBM Tealeaf cxImpact*.

Lorsque cette option est activée, la PCA capture les hits d'image avec le type de contenu suivant qui leur est associé :

```
Content-Type=image
```

Remarque :

- Les autres contenus statiques, comme les feuilles de style et le contenu JavaScript, sont au format de texte automatiquement capturé par IBM Tealeaf Application de capture passive CX.
  - Lorsqu'un serveur TLI est déployé, ces objets sont transférés de la PCA vers le pipeline de Windows. Dans le pipeline de Windows, l'agent de session TLI les transfère vers le serveur TLI afin de les archiver. Voir section "Agent de session TLI" du *Manuel de configuration d'IBM Tealeaf CX*.
- Si les options `Enable TLI` et `Delete Images on PCA Side` sont désactivées, `Enable TLI` redéfinit et détermine le comportement de capture de la PCA. Voir «Suppression des images dans la PCA», à la page 110.
- Pour assurer la capture du contenu d'image dans votre environnement Tealeaf, appliquez ce paramètre à partir des onglets Pipeline de toutes les instances de la PCA.

Lorsque le serveur Windows reçoit le hit, il examine la valeur `TLIHit` et, puisqu'elle est définie sur `True`, il transfère le hit vers le serveur TLI pour stockage dans l'archive appropriée.

- Les informations d'horodatage sont conservées avec le hit. Elles permettent par la suite au serveur TLI de fournir la version de l'image vue par le visiteur et enregistrée de façon à correspondre à la session du visiteur.
- Les hits envoyés sur le serveur TLI ne sont pas stockés dans le canister. Les données de session sont modifiées pour faire référence au contenu du serveur TLI à partir duquel plusieurs sessions peuvent interroger une entité unique stockée. Cette méthode réduit considérablement les coûts en matière de stockage.

Pour cette fonction, reportez-vous à la liste des extensions de fichier incluses et exclues. Si la fonction est activée ET :

- si l'extension de fichier figure dans la liste des extensions de fichier autorisées, la PCA traite le hit comme un type de capture standard pris en charge par la PCA. L'application capture la demande et la réponse puis marque l'objet image à l'aide des valeurs suivantes pour le serveur TLI :
  ```
  CaptureType=1
  TLIHit=False
  ```
- si l'extension de fichier ne figure pas dans la liste des extensions de fichier incluses, la PCA capture uniquement l'image objet. Elle le marque à l'aide des propriétés suivantes pour le serveur TLI :
  ```
  CaptureType=3
  TLIHit=True
  ```
- si l'extension de fichier figure dans la liste des extensions de fichiers exclues, la PCA capture uniquement l'objet image et le marque comme indiqué précédemment.

  Remarque : lorsque cette fonction est activée, les objets image sont toujours capturés, que l'objet figure ou non dans la liste des extensions de fichiers.
  - Si l'extension de fichier apparaît dans la liste des extensions de fichier autorisées, la PCA traite normalement le hit. Voir «Extensions de fichier autorisées», à la page 116.
  - Voir «Extensions de fichier exclues», à la page 116.

Listes des types de capture

Par défaut, la PCA est configurée pour capturer des types de données utiles à la plupart des applications Web. Le flux de capture peut contenir des types de données personnalisées et des extensions de fichier, tout particulièrement dans le cas des applications Internet enrichies.

- De plus, la PCA décompresse automatiquement les demandes POST à l'aide de types de codage de contenu et peut être configurée pour décompresser d'autres types de demande. Voir «Capture de la totalité des types de codage de contenu», à la page 117.

  Remarque : lorsque vous mettez à niveau la PCA, vous devez consulter la liste de tous les types de capture afin de vous assurer que tous les types de données nécessaires sont correctement capturés et traités.

Remarque : pour toutes les applications Web, vérifiez l'ensemble des types de capture de la PCA afin que les données significatives soient capturées et traitées par Tealeaf. Les données ne devant pas être capturées par IBM Tealeaf Application

de capture passive CX sont abandonnées et créent des hits abandonnés qui s'affichent dans les données de session.

Select view: Pipeline Settings | Edit Type Lists

Excluded File Extensions:

Add

au
avi
bin
bmp
cab

Remove selected

Included File Extensions:

Add

action

Remove selected

Capture All Mimetypes:

Add

application/json
application/x-json
application/xhtml+xml
text/json
text/x-json

Remove selected

Capture All POST types:

Add

Remove selected

XML POST types:

Add

Remove selected

Binary POST types:

Add

Remove selected

Capture All Content-Encoding types:

Add

Remove selected

Save changes | Revert changes

Figure 31. Listes des types de capture

Dans les sections des listes des types de capture, vous pouvez configurer des paramètres d'inclusion et des d'exclusion appliqués aux demandes et aux réponses. Par exemple, si vous supprimez le type de contenu `text/json` du panneau XML POST, le type de contenu est toujours capturé par défaut, mais le contenu n'est plus inséré dans la section `[xml1]`. Voir «Exemples JSON», à la page 115.

Remarque : après l'ajout de nouveaux types de contenu pour la capture, vous devez également les ajouter à l'aide de TMS si vous souhaitez indexer les réponses HTTPS du type capturé. Reportez-vous au chapitre relatif à la configuration de l'indexation CX dans le document *IBM Tealeaf CX Configuration Manual*.

Mode d'évaluation de la PCA pour les types de capture

Lorsque les hits sont identifiés dans l'onglet **Pipeline**, la PCA évalue le hit dans l'ordre suivant afin de déterminer s'il doit être capturé :

1. Demande :
   a. Vérifie la demande pour le type de codage de contenu. Si le type correspond à l'ensemble des types spécifiés pour la décompression, la demande est décompressée pour le traitement. Voir «Capture de la totalité des types de codage de contenu», à la page 117.
   b. Vérifie la demande pour les types de contenu suivants connus en interne. Voir «Types de contenu capturés par défaut», à la page 115.
   c. Définir le contenu de la demande et les types de corps :
      1) Vérifie la liste Type POST XML pour les POST de type XML à capturer. Voir «Types de POST XML», à la page 116.
      2) Vérifie la liste Type POST binaire pour les POST de type binaire à capturer. Voir «Types de POST binaires», à la page 117.
   d. Vérifiez la liste des extensions de fichier pour les types inclus et exclus :
      - Voir «Extensions de fichier autorisées», à la page 116.
      - Voir «Extensions de fichier exclues», à la page 116.
2. Réponse :
   a. Vérifiez les valeurs des listes de types de contenu suivantes :
      - «Capture de la totalité des types de POST», à la page 116
      - «Types de POST binaires», à la page 117
      - «Capturer tous les types Mime», à la page 116
   b. Si elle ne trouve aucune valeur dans les listes, la PCA vérifie sa liste par défaut interne des types de réponses. Voir «Types de réponse internes», à la page 115.
   c. Si les listes contiennent des valeurs, vérifiez les listes suivantes dans l'ordre indiqué.
3. Corps de demande : si la demande et la réponse réussissent les tests d'inclusion précédents, le corps de demande est traité.
   a. Si le type de contenu de la demande est défini dans l'un des cas précédents, la PCA traite son type de manière appropriée.
   b. Si le type de contenu pour le corps de demande est toujours inconnu après les vérifications précédentes, il vérifie la liste Capturer tous les types de POST.
      1) Si la liste contient le type de contenu, la PCA traite le corps comme du texte dans la section `[RequestBody]` de la demande générée.
      2) Voir «Capture de la totalité des types de POST», à la page 116.

Exemples JSON

JSON est une nouvelle norme utilisée dans de nombreuses applications Web. Certains modules Tealeaf, comme Tealeaf Logging Frameworks d' IBM Tealeaf CX Mobile, utilisent des POST JSON afin de soumettre les données du client à Tealeaf afin de les capturer. Les exemples de types de contenu suivants peuvent s'afficher dans Tealeaf, ou les données d'application.

Type de demande
: **Evaluation du type de contenu par la PCA**

`text/json`
: La demande est considérée comme un type de contenu de texte connu. Lorsque le traitement du corps de demande est achevé, il devient un type de contenu connu et est traité en tant que tel.

`application/json`
: Si le type de contenu de la demande est `application/json` et qu'il n'est pas défini dans la liste Capturer tous les types de POST, la PCA ne le reconnaît pas. Le corps de demande n'est pas traité et le hit est abandonné.

`application/json`
: Si le type de contenu de la demande est `application/json` et qu'il est défini dans la liste Capturer tous les types de POST, la PCA le reconnaît. S'il n'est pas répertorié dans les listes de types XML ou binaire, il est considéré comme un type texte et est traité comme du texte.

Pour plus d'informations sur le schéma JSON Tealeaf, utilisé pour capturer le contenu des environnements de capture des clients, voir section "Référence du schéma de l'objet JSON de Tealeaf" du *Guide d'intégration des données des environnements de capture des clients d'IBM Tealeaf*.

Types de contenu capturés par défaut

Par défaut, la PCA capture les types de contenu suivants.

Remarque : Ces types de contenu sont définis par défaut dans la PCA et ne nécessitent aucune configuration pour la capture.

Types de demandes internes par défaut

- `application/x-www-form-urlencoded`
- `application/xml`
- `multipart/form-data`
- `text/*`
- `text/xml`

Types de réponse internes

Remarque : cette liste s'applique aux types de contenu des réponses. Les types de contenu des demandes sont évalués selon l'ordre défini. Voir «Mode d'évaluation de la PCA pour les types de capture», à la page 114.

- `text/*`
- `application/text/*`

Extensions de fichier exclues

Indique les extensions de fichier à exclure du DataStream capturé. Il est possible d'utiliser ce paramètre pour affiner le comportement défini selon le mode de capture.

Remarque : par défaut, la PCA ne capture par les fichiers JavaScript. Si votre application Web génère des fichiers JavaScript dynamiques et que vous souhaitez les capturer, vous devez les ajouter manuellement à l'ensemble des types capturés.

Extensions de fichier autorisées

Indique les extensions de fichier entièrement capturées. Il est possible d'inclure les fichiers binaires comme les PDF.

Remarque : si vous déployez un serveur TLI pour la capture de contenu statique, vous devez insérer les extensions de fichier des types de contenu statique dans cette zone afin de les capturer et les insérer dans le serveur TLI. Voir section "Gestion des archives statiques" du *Manuel d'administration d'IBM Tealeaf cxImpact*.

Capturer tous les types Mime

Spécifie les types de contenu de réponse (types MIME) pour lesquels capturer un hit complet.

Capture de la totalité des types de POST

Spécifie les types de contenu dans les données de demande ne faisant pas partie des données standard XML ou des données de formulaire.

Types de POST XML

Dans cette section, vous pouvez définir les types de POST XML à ajouter à la demande. Lorsqu'une correspondance est trouvée pour le type de contenu XML spécifié, la section `[xml1]` est ajoutée à la mémoire tampon de la demande et le contenu y est inséré.

Remarque : Les nouvelles installations de la PCA à partir de la build 3324 sont automatiquement configurées pour capturer les types de POST XML répertoriés. Ces types de POST XML ont été ajoutés à la build 3324 de la PCA. Si vous utilisez une build antérieure ou une version mise à niveau à partir d'une build antérieure, vous devez configurer manuellement ces types de capture.

Par défaut, certains types de contenu sont automatiquement contrôlés et capturés. Il ne faut pas les ajouter. Voir «Types de contenu capturés par défaut», à la page 115.

Selon le type de kit d'outils JSON, les types de contenu ci-dessous peuvent s'afficher dans le flux de capture. S'ils sont présents, ces types doivent être ajoutés.

- `application/x-javascript`
- `text/javascript`
- `text/x-javascript`
- `text/x-json`

Types de POST binaires

Il est possible de configurer la PCA pour capturer des types de POST binaires. Par exemple, les applications basées sur AMF soumettent des demandes binaires au serveur Web. Pour capturer des données de requête AMF, ajoutez `application/x-amf` à la liste.

- Par défaut, la PCA ne capture pas les réponses binaires.
- Le décodage des données AMF doit être activé dans le pipeline de Windows. Voir section "Agent de session de déploiement" du *Manuel de configuration d'IBM Tealeaf CX*.

Lorsque `application/x-tlt-ld` est activé pour la capture, les demandes de tous les hits capturés de ce type possèdent la variable de demande suivante, insérée dans la section `[env]` :

```
PostRequestBodyEncoding=Base64
```

Pour les autres hits, cette valeur est définie sur `None`.

Remarque : Dans la version 8.4 ou supérieure, la capture du fichier post binaire `application/x-tlt-d` est obsolète. Voir .

Capture de la totalité des types de codage de contenu

Dans PCA build 3502 et supérieure, vous pouvez spécifier les types de codage de contenu à l'aide d'une zone de texte dont les demandes sont déployées lors du processus de capture.

Remarque : Dans PCA build 3502 et supérieure, les types de codage de contenu suivants sont automatiquement décompressés et ne doivent pas être spécifiés ici :

- `*/deflate`
- `*/gzip`
- `*/x-gzip`

Lorsqu'une demande reçue par la PCA correspond à l'un des types de codage spécifiés, la PCA décompresse ou extrait automatiquement la demande.

Le tableau suivant décrit les comportements :

Tableau 3. Capturer tous les types de codage de contenu

Dans d'autres listes de type de capture ?	Dans Capturer tous les types de codage de contenu ?	Capturé ?	Décompressé ?	Remarques
O	O	O	O	`*/deflate`, `*/gzip`, et `*/x-gzip` sont automatiquement décompressés.
N	O	N	N	abandonné
O	N	O	N*	capturé ; non décompressés (* sauf s'il s'agit d'un des types de codage de contenu décompressés par défaut)
N	N	N	N	abandonné

Types de contenu et indexation

Après que la PCA a capturé le contenu, la demande et la réponse de chaque hit sont envoyées vers un canister pour un traitement supplémentaire, y compris l'indexation du contenu pour la recherche.

- Requête : les sections spécifiques de la demande sont automatiquement indexées pour la recherche. Voir section "Configuration de CX Indexing" du *Manuel de configuration d'IBM Tealeaf CX*.
  - Vous pouvez configurer des règles de confidentialité afin de déplacer le contenu d'une section de la demande à une autre section indexée automatiquement. Nous vous recommandons d'appliquer ces règles de confidentialité au canister. Voir section "Agent de session de confidentialité" du *Manuel de configuration d'IBM Tealeaf CX*.
- Réponse : si vous le souhaitez, vous pouvez ajouter des types de réponses HTTP individuels pour l'indexation. Voir section "Configuration de CX Indexing" du *Manuel de configuration d'IBM Tealeaf CX*.

Téléchargement de la configuration de confidentialité

Si nécessaire, vous pouvez télécharger le fichier de configuration de la confidentialité `privacy.cfg` vous permettant d'effectuer des modifications et d'archiver en étant hors ligne à partir de l'onglet Sauvegardes/journaux.

Remarque : `privacy.cfg` doit être mis en forme dans un format compatible avec UTF-8.

L'onglet **Sauvegardes/journaux** contient deux sections :

Remarque : la console Web de la PCA peut conserver jusqu'à cinq versions du fichier `privacy.cfg`. Voir «Modifications de la confidentialité», à la page 136.

- Dans la section **Fichier de configuration de la confidentialité**, cliquez sur **Télécharger la sélection**.
- Dans la section **Journaux**, cliquez sur le lien **fichiers de configuration**.
- Voir «Console Web de la PCA - Onglet Journaux de sauvegarde», à la page 159.

Manipulation des règles

Commande
: **Description**

`Insert Rule 1`
: Permet d'insérer une nouvelle règle à appliquer en premier et de charger la page Modifier la règle.

`Enable/Disable`
: Permet d'activer ou de désactiver la règle de la ligne.

`Delete`
: Permet de supprimer de la session la règle de la ligne. Pour que le fichier `privacy.cfg` soit modifié, il est nécessaire d'enregistrer les modifications.

`Edit`
: Permet de charger la page Modifier pour cette règle.

`Insert Below`
: Permet d'insérer une nouvelle règle en dessous de la ligne et de charger la page Modifier la règle.

`arrows`
: Permet de déplacer la règle vers le haut ou vers le bas selon la flèche utilisée. Les règles sont appliquées dans l'ordre et doivent être modifiées.

Les modifications effectuées à l'aide des flèches sont appliquées dans la session. Pour les enregistrer, cliquez sur **Enregistrer les modifications**.

Manipulation des tests

Commande
: **Description**

`Add`
: Permet de charger la page Ajouter un test.

`Edit`
: Permet de charger la page Modifier pour le test en question.

Manipulation de l'action

Commande
: **Description**

`Add`
: Permet de charger la page Ajouter une Action.

`Delete/In Use`
: Si l'action peut être supprimée, un lien Supprimer est disponible dans la colonne Actions à effectuer.
  - Si l'action est indiquée comme étant en cours d'utilisation, une règle fait référence à l'action et il n'est pas possible de la supprimer. Pour supprimer une action en cours, il est nécessaire de supprimer toutes les références à l'action contenues dans les règles. Vous pouvez voir les actions en cours d'utilisation dans la colonne Actions à effectuer du tableau Règles.

`Edit`
: Permet de charger la page Modifier pour une action spécifique.

Manipulation des clés

Commande
: **Description**

`Add`
: Charge la page Ajouter une clé.

`Delete`
: Supprime la clé.

`Edit`
: Charge la page Modifier pour cette clé.

L'ajout d'une clé est facultatif et permet de définir clairement des clés de confidentialité ainsi que leur valeur (chiffrée). En règle générale, une clé est ajoutée lorsqu'un filtre de confidentialité est exécuté sur une autre machine que le serveur IBM Tealeaf CX (par exemple sur un serveur Web) où les clés de confidentialité définies ne sont pas directement accessibles. Les entrées de cette section doivent être au format suivant :

```
keyID=keydata
```

où :

- `dkeyID` représente le nom (ID) de la clé
- `keydata` représente la chaîne de la valeur de clé chiffrée

Ajout/modification de règles

Rule Details

Name:	Rule1
Description:	Block URL Fields
ReqField:	None Selected
ReqOp:	None Selected
ReqVal:	
TestOp:	None Selected
List Delimiter	
Case Sensitive	
ReqValIsField	
Not (logical NOT)	
Stop Processing	
Enabled	

Actions:

TextBlockURLFields

[Drop1] add

remove selected

Tests:

AnotherTest

add

remove selected

Figure 32. Page Ajouter/modifier les règles

Pour définir une condition unique (test), vous pouvez renseigner les zones ReqField, ReqOp, et ReqVal dans une règle. Pour des conditions plus complexes, utilisez l'option Tests et définissez séparément les conditions du test.

Paramètre
: **Description**

`Nom`
: Nom de la règle

`Description`
: Dans cette zone, l'utilisateur peut lire une description de l'action ; elle est également affichée dans `privacy.cfg`.

`ReqField`
: Cette option définit le nom d'une zone, la partie nom d'une paire nom-valeur dans le fichier de demande. La valeur de cette zone est utilisée à titre comparatif. Vous pouvez également appliquer un des noms de zone spéciaux suivants :

- `TL_URLEXT` : représente la partie de l'extension de fichier de l'URL

- veTL_URLTAIL : représente l'extrémité de l'URL, y compris le dernier signe / de l'URL et tout ce qui vient après
- TL_VIRTUALDIR : représente la partie du répertoire virtuel de l'URL

ReqOp ReqOp définit l'opération de comparaison effectuée par cette règle entre ReqField et ReqVal. Voici les valeurs valides pour cette option :

- EQ ou = : True lorsque la valeur de zone est égale à ReqVal. La comparaison des chaînes est insensible à la casse.
- NE ou != : True lorsque la valeur de zone n'est pas égale à ReqVal. La comparaison des chaînes est insensible à la casse.
- GT ou > : True lorsque la valeur de zone est supérieure à ReqVal.
- LT ou < : True lorsque la valeur de zone est inférieure à ReqVal
- CONTAINS : True lorsque la valeur de zone contient ReqVal.
- PARTOF : True lorsque la valeur de zone fait partie de (est contenue dans) ReqVal
- PARTOFLIST : True lorsque la zone de valeur correspond à une des valeurs de ReqVal.
  - Vous pouvez utiliser des points-virgules, ou tout autre délimiteur spécifié par la propriété ListDelimiter, pour délimiter la liste des valeurs dans ReqVal.

ReqVal

Indique une valeur littérale ou un nom de zone (définir ReqValIsField=True pour le nom de zone). Lorsque ReqOp=PARTOFLIST, ce paramètre doit indiquer une liste de valeurs séparées par des points-virgules ou tout autre délimiteur (spécifié par le biais de ListDelimiter).

- Si ReqField est défini sur TL_URLEXT, cette zone contient les extensions comprenant des points.

TestOp

Il s'agit de l'opérateur logique à utiliser lorsque plusieurs tests sont spécifiés. Vous pouvez choisir entre AND et OR. Si aucune valeur n'est spécifiée, AND est appliquée comme valeur par défaut.

- Lorsque TestOp=AND, tous les tests doivent renvoyer True afin de pouvoir effectuer les actions.
- Lorsque TestOp=OR, les actions sont effectuées si un des tests renvoie True.

Délimiteur de liste

Indique le caractère de séparation des éléments de liste dans ReqVal lorsque ReqOp=PARTOFLIST est utilisé. Par défaut, il s'agit d'un point-virgule (;).

Sensible à la casse

Valeur True ou False indiquant si les recherches des noms de zone doivent être sensible à la casse. La valeur par défaut est False. Les recherches sont plus rapides lorsque vous la définissez sur True.

ReqValIsField

Valeur True ou False indiquant si ReqVal contient un nom de zone.

Not Valeur True ou False. Si la valeur est définie sur True, le résultat du test est inversé (opérateur logique NOT).

Arrêter le traitement
Valeur `True` ou `False` indiquant s'il est nécessaire d'interrompre le traitement de règles supplémentaires si la règle est définie sur `True`.

Activé
Valeur `True` ou `False` définissant si la règle est active.

Actions
Cette zone contient un ou plusieurs noms d'action correspondant aux noms des sections d'action à effectuer si la règle renvoie `True`.

Tests
Cette zone contient un ou plusieurs noms de test correspondant aux noms des sections de test. Les tests spécifiés sont évalués afin de déterminer si les actions sont exécutées pour la règle. Si aucun test n'est spécifié (ni aucun test intégré comme décrit ci-dessous) les actions sont exécutées pour tous les hits.

Ajout/modification de tests

Test Details
Name: SampleTest1
Description: A sample test
ReqField: ...(enter in field to right) StatusCode
ReqOp: partoflist
ReqVal: 200
List Delimiter:
ReqValIsField
Case Sensitive
Not (logical NOT)

Figure 33. Page Ajouter/modifier des tests

Paramètre
Description

Nom
Indique le nom du test.

Description
Dans cette zone, l'utilisateur peut lire une description du test qui apparaît également dans `privacy.cfg`.

ReqField
Partie nom d'une paire nom-valeur. Il peut également s'agir d'un des noms réservés suivants :

- `TL_URLEXT`
- `TL_URLTAIL`
- `TL_VIRTUALDIR`

ReqOp
Indique l'opération à effectuer. Vous pouvez choisir parmi les options suivantes :

- `EQ` ou `=`

- NE ou != ou <>
- GT ou >
- LT ou <
- CONTAINS
- PARTOF
- PARTOFLIST

ReqVal
Indique une valeur littérale ou un nom de zone (définir ReqValIsField=True pour le nom de zone). Lorsque ReqOp=PARTOFLIST, cette valeur doit indiquer une liste de valeurs séparées par des points-virgules ou tout autre délimiteur (spécifié par le biais de ListDelimiter).

ListDelimiter
Indique le caractère de séparation des éléments de liste dans ReqVal lorsque ReqOp=PARTOFLIST. Par défaut, il s'agit d'un point-virgule (**;**).

ReqValIsField
Valeur True ou False indiquant si ReqVal contient un nom de zone.

CaseSensitive
Valeur True ou False indiquant si les recherches des noms de zone doivent être sensibles à la casse. La valeur par défaut est False. Les recherches sont plus rapides lorsque vous la définissez sur True.

Not Valeur True ou False. Si la valeur est définie sur True, le résultat du test est inversé (opérateur logique NOT).

Ajouter/modifier des actions

Action Details

Name:	DropHit		
Description:	Drop the Hit		
Referenced By Rule:	2	Section:	None Selected
Invert Action:	☐		
Action:	DropHit	Field:	
Key:	None Selected	Value Name:	
Start Pattern:		Start Pattern RE:	
End Pattern:		End Pattern RE:	
Strike Character:		Inclusive:	☐
Strike Length (optional):		Repeat Count:	
Blocking Mask (optional):		Replace String:	
Length (bytes):		Case Sensitive:	☐
Ignore Special:	☐	ReqSetResult:	
ReqSetSection:		ReqSetField:	

Figure 34. Page Ajouter/modifier des actions

En haut de la page Détails de l'action, vous pouvez modifier le nom de l'action et les règles dans lesquelles elle se trouve ainsi que la configuration actuelle des propriétés.

Paramètre
: **Description**

`Nom`
: Indique le nom de l'action.

`Description`
: Dans cette zone, l'utilisateur peut lire une description de l'action ; elle est également affichée dans `privacy.cfg`.

`Inverser l'action`
: Valeur `True` ou `False` indiquant s'il est nécessaire d'inverser l'action (à effectuer pour toutes les zones ou noms de valeur SAUF ceux qui sont spécifiés).

- Lorsque la zone Value Name est spécifiée, tous les noms sauf ceux indiqués dans cette zone sont traités.
- Lorsque la zone Value Name n'est pas spécifiée, les noms indiqués dans la zone Field sont exclus de l'action.

Remarque : Cette action peut être uniquement utilisée avec les actions `Block`, `Encrypt`, et `Replace`.

Les actions Start Pattern et Start Pattern RE ne peuvent pas être utilisées avec une action d'inversement.

Action
Désigne l'action à effectuer. Il peut s'agir d'une des valeurs suivantes :
- Block : permet de verrouiller les données correspondantes à l'aide du caractère de substitution spécifié.
- Encrypt : permet de chiffrer et de masquer les données correspondantes à l'aide du caractère de substitution spécifié.
- Replace : permet de remplacer les données correspondantes par une chaîne de texte spécifiée.
- DropHit : permet de supprimer le hit en cours (aucune autre action n'est effectuée).
- DropResponse : permet de supprimer la réponse du hit en cours.
- ReqSet : permet de définir ou de remplacer la valeur de la paire nom-valeur dans la demande. Si elle n'existe pas, la paire nom-valeur est créée ; il est en de même pour la section spécifiée.
- ReqAppend :s'ajoute à la valeur de la paire nom-valeur spécifiée dans la demande. Si elle n'existe pas, la paire nom-valeur est créée ; il est en de même pour la section spécifiée.
- ReqDelete : permet de supprimer de la demande la totalité de la paire nom-valeur spécifiée. Cette action ne supprime pas la section, même lorsqu'elle est vide.

Clé ID clé à utiliser lorsque Action=Encrypt.

Section
Indique le nom de la section des données sur lesquelles agir. Si la valeur est définie sur response, la réponse est traitée. Il peut également s'agir d'un des noms réservés suivants :
- urlfield : permet d'effectuer l'action pour les noms de valeur spécifiés (ou tout si la zone Value Name n'est pas définie) pour les valeurs de la section urlfield, c'est-à-dire QUERY_STRING, de la chaîne de requête de RawRequest (le cas échéant), la chaîne de requête de HTTP_REFERER ainsi que de l'en-tête et le corps de demande du référenceur de RawRequest (le cas échéant).
- cookies : permet d'effectuer l'action pour les noms de valeur spécifiés (ou tout si la zone Value Name n'est pas définie) pour les valeurs de la section [cookies], c'est-à-dire les paires nom-valeur HTTP_COOKIE et HTTP_SET_COOKIE, des en-têtes de paramétrage des cookies dans la section ResponseHeader (le cas échéant), les en-têtes de paramétrage des cookies dans la réponse et dans l'en-tête [cookies] de la section RawRequest (le cas échéant).

  Remarque : Lorsqu'une section n'est pas spécifiée dans une action, la totalité de la mémoire tampon de requête est utilisée.

Zone Indique un ou plusieurs noms de zone facultatifs (partie nom de la paire nom-valeur. Lorsque Field et Value Name ne sont pas définis, la section entière est verrouillée/chiffrée. Il peut également s'agir d'un des noms réservés suivants :
- body : lorsque Section=response, cette valeur définit le corps de réponse comme cible. Lorsque Section=RawRequest, le corps de demande (le cas échéant) est traité.

Nom de valeur
Indique un ou plusieurs noms de valeurs (dans des paires nom-valeur à valeurs multiples comme HTTP_COOKIE) ou les noms des éléments lorsque `Section=urlfield` ou `Section=cookies`.

Modèle de début
Indique le modèle de chaîne de début à rechercher dans les données spécifiées. Les données qui suivent immédiatement le modèle correspondant sont traitées. Si la zone `Start Pattern` est utilisée, vous devez également spécifier la zone `End Pattern` ou `Strike Length`, à moins de définir `Inclusive=True`. Lorsque cela est défini, les actions `Start Pattern` et, facultativement, `End Pattern` sont également verrouillées/chiffrées. Cette action est utile lorsque vous souhaitez verrouiller ou chiffrer une chaîne de données constantes.

Modèle de début RE
Il s'agit de la version d'expression régulière de `Start Pattern`. Vous pouvez utiliser cette action pour spécifier une expression régulière standard afin de définir le modèle de début à rechercher. Vous pouvez utiliser `Start Pattern` ou `Start Pattern RE`, mais pas les deux.

Modèle de fin
Représente le modèle de chaîne qui indique la fin des données identifiées par une action `Start Pattern`. Les données jusqu'à `End Pattern` (non inclus) sont traitées (sauf si `Inclusive=True`).

Modèle de fin RE
Il s'agit de la version d'expression régulière de `End Pattern`. Vous pouvez utiliser cette action pour spécifier une expression régulière standard afin de définir le modèle de fin à trouver. Vous pouvez utiliser `End Pattern` ou `End Pattern RE`, mais pas les deux.

Caractère de remplacement
Indique le caractère utilisé pour remplacer les données d'origine verrouillées ou chiffrées. Il peut s'agir de n'importe quel caractère alphanumérique ou symbole, excepté ceux de la liste suivante :

- . (point)
- , (virgule)
- / (barre oblique)
- \ (barre oblique inversée)
- [(crochet gauche)
-] (crochet droit)
- | (barre verticale)
- ' (guillemet simple)
- " (guillemet double)

Longueur de biffage
Indique la taille en octets des données de substitution (facultatif). Il s'agit du nombre de caractères indiqués dans la zone Strike Character utilisés pour remplacer les données d'origine (lorsque `Action=Block` ou `Action=Encrypt`).

- Si la valeur indiquée dans `Strike Length` est plus grande que les données d'origine, des caractères de substitution supplémentaires sont ajoutés.

- Si la valeur de Strike Length est plus petite que la taille des données d'origine, les caractères de la zone Strike Length sont remplacés par le contenu de la zone Strike Character et les données restantes sont supprimées.
- Si la valeur de Strike Length est un nombre négatif, le nombre de caractères représentés par la valeur absolue de la zone Strike Length reste inchangé. Par exemple, pour conserver les quatre derniers caractères ou une valeur, définissez Strike Length=-4. Voir Blocking Mask pour plus d'options de verrouillage flexibles.

Inclusif
: Valeur True ou False indiquant si Start Pattern (ou Start Pattern RE) et, facultativement, End Pattern (ou End Pattern RE) sont verrouillés ou chiffrés. La valeur par défaut est False.

Comptage de répétition
: Peut être utilisée pour les actions bénéficiant d'une action Start Pattern ou Start Pattern RE afin de définir le nombre d'instances de données à traiter correspondant au modèle.

Masque de blocage
: Représente une expression régulière spécifiant les caractères des données trouvées à remplacer par le caractère de substitution (ne s'applique pas à l'action Replace). Tous les caractères d'un groupe (défini entre parenthèses) de l'expression régulière sont remplacés par le caractère de substitution.

- Les caractères correspondant à une partie du modèle situés en dehors d'un groupe ne sont pas remplacés. Par exemple, le masque suivant verrouille uniquement les chiffres d'un numéro de sécurité social, en laissant apparaître les tirets :

  ```
  BlockingMask=([0-9]{3})-([0-9]{2})-([0-9]{4})
  ```

  Ici, seuls les quatre premiers chiffres d'une carte de crédit sont visibles :

  ```
  BlockingMask=[0-9]{4}([0-9]*)
  ```

  Blocking Mask est utilisé à la place de Strike Length. Vous pouvez utiliser l'un ou l'autre, mais pas les deux.

  Remarque : Faites attention lorsque vous utilisez Blocking Mask. Si les données ne correspondent pas à l'expression régulière spécifiée pour Blocking Mask, elles ne seront ni verrouillées ni chiffrées.

Chaîne de remplacement
: Représente la chaîne utilisée pour remplacer les données d'origine lorsque Action=Replace.

Longueur (octets)
: Utilisée à la place d'une action End Pattern ou End Pattern RE, cette valeur indique la taille des données (en octets) à traiter suivant une action Start Pattern (ou Start Pattern RE) correspondante.

Sensible à la casse
: Valeur True ou False indiquant si les recherches des noms de zone et/ou des modèles doivent être sensibles à la casse. La valeur par défaut est False. Les recherches sont plus rapides lorsque vous la définissez sur True.

Ignorer manipulation spéciale
: Valeur True ou False indiquant s'il est nécessaire ou non d'ignorer une manipulation spéciale lorsque urlfield ou cookies est défini pour la

section. Si la valeur est définie sur `True`, les actions `Start Pattern` ou `Start Pattern RE` peuvent être utilisées dans les sections `urlfield` ou `cookies`. La valeur par défaut est `False`.

`ReqSetSection`
Définit la section pour la paire nom-valeur d'une action `ReqSet`, `ReqAppend`, ou `ReqDelete`. `ReqSetSection` est obligatoire pour ces trois actions.

`ReqSetField`
Indique le nom d'une paire nom-valeur pour une action `ReqSet`, `ReqAppend`, ou `ReqDelete`. `ReqSetField`est obligatoire pour ces trois actions.

`ReqSetResult`
Cette option est utilisée en association avec `Start Pattern RE` afin de produire une valeur formatée pour une action `ReqSet` ou `ReqAppend`. L'expression `Start Pattern RE` doit contenir un ou plusieurs "groupes" définis entre parenthèses dans l'expression régulière. `ReqSetResult` représente une chaîne contenant un texte littéral et des paramètres de substitution pour les données capturées par `Start Pattern RE`. Par exemple :

```
StartPatternRE=name="(.*?)" value="(.*?)"
ReqSetResult=Field
{g1} value: {g2}
```

Voici le résultat de ce code :

```
Field name value: Bob
```

Le premier paramètre de substitution, {g1}, est remplacé par la valeur du premier groupe dans l'expression régulière. {g2} représente la deuxième valeur, et ainsi de suite. La chaîne de résultat est ensuite utilisée comme valeur pour l'action `ReqSet` ou `ReqAppend`.

Ajout/modification de clés

Les clés de confidentialité peuvent être générées dans Tealeaf pour chiffrer et déchiffrer des données sensibles dans le système. Le chiffrement et le déchiffrement sont gérés par le filtre de confidentialité disponible dans la PCA et dans le pipeline de Windows.

- Pour plus d'informations sur la confidentialité du pipeline, voir section"Agent de session de confidentialité étendue" du *Manuel de configuration d'IBM Tealeaf CX*.
- Pour plus d'informations sur la création de règles de pipeline, voir chapitre "Agent de session de confidentialité" du *Manuel de configuration d'IBM Tealeaf CX*.
- Pour une présentation générale de la manière dont Tealeaf gère la confidentialité, voir chapitre "Gestion de la confidentialité des données dans Tealeaf CX" du *Manuel d'installation d'IBM Tealeaf CX*.

Les clés de confidentialité utilisées pour chiffrer et déchiffrer des données sensibles dans Tealeaf doivent être ajoutées dans la console Web de la PCA.

Remarque : Toute clé de chiffrement utilisée par la PCA pour chiffrer et par le serveur de recherche pour déchiffrer doit être définie dans la configuration du serveur de recherche et fournie à la PCA. Pour plus d'informations sur la définition des clés, voir chapitre "Configuration du serveur de recherche" du *Manuel de configuration d'IBM Tealeaf CX*.

Vous pouvez ajouter des clés de confidentialité pour la PCA à utiliser lors des opérations de chiffrement effectuées par le filtre de confidentialité dans la PCA. Afin que la clé de confidentialité fonctionne dans la PCA, entrez le nom de la clé et la clé générée dans cette section.

- Vous pouvez copier une valeur de clé générée à partir de la configuration du serveur de recherche et la coller dans les zones de texte répertoriées.

Key Details

Name:

Key:

Figure 35. Page Ajout/modification de clés

Paramètre
Description

Nom Nom de la clé

Clé La clé proprement dite

Références du fichier `Privacy.cfg`

Cette section contient une présentation des références du fichier `Privacy.cfg` utilisé pour configurer les règles de confidentialité appliquées au flux de capture dans IBM Tealeaf Application de capture passive CX.

Remarque : évitez d'effectuer des modifications directement dans ce fichier de configuration. Nous vous conseillons de modifier votre configuration de la confidentialité à partir de l'onglet **Règles** de la console Web, car il fournit une interface utilisateur pour ce fichier de configuration. Pour plus d'informations, voir «Navigateurs pris en charge pour la console Web de la PCA», à la page 54.

La confidentialité permet de supprimer ou de chiffrer les informations sensibles du flux de capture. Vous pouvez appliquer des règles de confidentialité aux éléments suivants lors de la capture et du traitement des données de session.

1. IU de capture
2. PCA
3. Pipeline de Windows
   voir section "Gestion de la confidentialité des données dans Tealeaf CX" du *Manuel d'installation d'IBM Tealeaf CX*.

Vous pouvez utiliser l'utilitaire de test de la confidentialité de Windows afin de développer et de tester vos règles de confidentialité. Il est ensuite possible de les coller à nouveau dans le fichier de configuration pour les appliquer dans la PCA.

- Voir section "Utilitaire de test de la confidentialité" du *Manuel de configuration d'IBM Tealeaf CX*.

Vous trouverez des informations supplémentaires dans les remarques du fichier de configuration `Privacy.cfg`. Ce dernier se situe dans le répertoire `/usr/local/ctccap/etc`. Vous pouvez le modifier à l'aide de l'éditeur vi.

Règles

Propriété
: **Description**

`Activé`
: Valeur `True` ou `False` indiquant si cette règle est active.

`Tests`
: Cette zone contient un ou plusieurs noms de test correspondant aux noms des sections de test. Les tests spécifiés sont évalués afin de déterminer si les actions sont exécutées pour la règle. Si aucun test n'est spécifié (ni aucun test intégré comme décrit ci-dessous) les actions sont exécutées pour tous les hits.

`TestOp`
: Il s'agit de l'opérateur logique à utiliser lorsque plusieurs tests sont spécifiés. Vous pouvez choisir entre `AND` et `OR`.
  - Lorsque `TestOp=AND`, tous les tests doivent renvoyer `True` afin de pouvoir effectuer les actions.
  - Lorsque `TestOp=OR`, les actions sont effectuées si un des tests renvoie `True`.

`Not`
: Valeur `True` ou `False`. Si la valeur est définie sur `True`, le résultat du test est inversé (opérateur logique `NOT`).

`StopProcessing`
: Valeur `True` ou `False` indiquant s'il est nécessaire d'interrompre le traitement de règles supplémentaires si la règle effectue l'évaluation en étant définie sur `True`.

`Actions`
: Cette zone contient un ou plusieurs noms d'action correspondant aux noms des sections d'action à effectuer si la règle renvoie `True`.

`ReqField`
: Affiche une partie du nom d'une paire nom-valeur. Il peut également s'agir d'un des noms réservés suivants :
  - `TL_URLEXT`
  - `TL_URLTAIL`
  - `TL_VIRTUALDIR`

`ReqOp`
: Indique l'opération à effectuer. Vous pouvez choisir parmi les options suivantes :
  - `EQ` ou `=`
  - `NE` ou `!=` ou `<>`
  - `GT` ou `>`
  - `LT` ou `<`
  - `CONTAINS`
  - `PARTOF`
  - `PARTOFLIST`

`ReqVal`
: Indique une valeur littérale ou un nom de zone (définir `ReqValIsField=True` pour le nom de zone). Lorsque `ReqOp=PARTOFLIST`, cette valeur doit indiquer une liste de valeurs séparées par un point-virgule ou tout autre délimiteur (spécifié par le biais de `ListDelimiter`).

`ReqValIsField`
: Valeur `True` ou `False` indiquant si `ReqVal` contient un nom de zone.

ListDelimiter
: Indique le caractère de séparation des éléments de liste dans `ReqVal` lorsque `ReqOp=PARTOFLIST`. Par défaut, il s'agit d'un point-virgule, **;**.

CaseSensitive
: Valeur `True` ou `False` indiquant si les recherches des noms de zone doivent être sensibles à la casse. La valeur par défaut est `False`. Les recherches sont plus rapides lorsque vous la définissez sur `True`.

Tests

Propriété
: **Description**

ReqField
: Affiche la partie nom d'une paire nom-valeur. Il peut également s'agir d'un des noms réservés suivants :
  - `TL_URLEXT`
  - `TL_URLTAIL`
  - `TL_VIRTUALDIR`

ReqOp
: Indique l'opération à effectuer. Vous pouvez choisir parmi les options suivantes :
  - `EQ` ou =
  - `NE` ou != ou <>
  - `GT` ou >
  - `LT` ou <
  - `CONTAINS`
  - `PARTOF`
  - `PARTOFLIST`

ReqVal
: Indique une valeur littérale ou un nom de zone (définir `ReqValIsField=True` pour le nom de zone). Lorsque `ReqOp=PARTOFLIST`, cette valeur doit indiquer une liste de valeurs séparées par des points-virgules ou tout autre délimiteur (spécifié par le biais de `ListDelimiter`).

ReqValIsField
: Valeur `True` ou `False` indiquant si `ReqVal` contient un nom de zone.

ListDelimiter
: Indique le caractère de séparation des éléments de liste dans `ReqVal` lorsque `ReqOp=PARTOFLIST`. Par défaut, il s'agit d'un point-virgule, **;**.

CaseSensitive
: Valeur `True` ou `False` indiquant si les recherches des noms de zone doivent être sensibles à la casse. La valeur par défaut est `False`. Les recherches sont plus rapides lorsque vous la définissez sur `True`.

Not
: Valeur `True` ou `False`. Si la valeur est définie sur `True`, le résultat du test est inversé (opérateur logique `NOT`).

Actions

Propriété
: **Description**

Action
: Désigne l'action à effectuer. Voici les valeurs :

- `Block` : permet de bloquer les données correspondantes à l'aide du caractère de substitution spécifié.
- `Encrypt` : permet de chiffrer et de masquer les données correspondantes à l'aide du caractère de substitution spécifié.
- `Replace` : permet de remplacer les données correspondantes par une chaîne de texte spécifiée.
- `DropHit` : permet de supprimer le hit en cours (aucune autre action n'est effectuée). Chaque règle peut posséder une action d'abandon des hits.
- `DropResponse` : permet de supprimer la réponse du hit en cours.
- `ReqSet` : permet de définir ou de remplacer la valeur de la paire nom-valeur dans la demande. Si elle n'existe pas, la paire nom-valeur est créée ; il en est de même pour la section spécifiée.
- `ReqAppend` : s'ajoute à la valeur de la paire nom-valeur spécifiée dans la demande. Si elle n'existe pas, la paire nom-valeur est créée ; il en est de même pour la section spécifiée.
- `ReqDelete` : permet de supprimer de la demande la totalité de la paire nom-valeur spécifiée. Cette action ne supprime pas la section, même lorsqu'elle est vide.

`Key` ID clé à utiliser lorsque `Action=Encrypt`.

`Group` Nom de groupe (au format domaine\nom du groupe) à utiliser pour le chiffrement lorsque `Action=Encrypt`.

Remarque : Utilisez `Key` ou `Group` pour indiquer la clé de chiffrement, mais pas les deux.

`Section`

Indique le nom de la section des données sur lesquelles agir. S'il s'agit d'une valeur définie sur `response`, alors la réponse est traitée. Il peut également s'agir d'un des noms réservés suivants :

- `urlfield` : permet d'effectuer l'action pour le ValueName spécifié (ou tout si ValueName n'est pas défini) pour les valeurs de la section urlfield, c'est-à-dire QUERY_STRING, de la chaîne de requête de RawRequest (le cas échéant), la chaîne de requête de HTTP_REFERER, l'en-tête de requête et le corps de demande du référenceur de RawRequest (le cas échéant).
- `cookies` : permet d'effectuer l'action pour le ValueName (ou tout si ValueName n'est pas défini) pour les valeurs de la section `[cookies]`, c'est-à-dire les paires nom-valeur HTTP_COOKIE et HTTP_SET_COOKIE, les en-têtes de paramétrage des cookies de la section ResponseHeader (le cas échéant), les en-têtes de paramétrage des cookies dans la réponse et l'en-tête `[cookies]` de la section RawRequest (le cas échéant).

  Remarque : Lorsqu'une section n'est pas spécifiée dans une action, la totalité de la mémoire tampon de requête est utilisée.

`IgnoreSpecial`

Valeur `True` ou `False` indiquant s'il est nécessaire ou non d'ignorer une manipulation spéciale lorsque `urlfield` ou `cookies` est défini pour la section. Si la valeur est définie sur `True`, `StartPattern` ou `StartPatternRE` peuvent être utilisés dans les sections `urlfield` ou `cookies`. La valeur par défaut est `False`.

`Field` Indique un ou plusieurs noms de zone facultatifs (partie nom de la paire

nom-valeur. Lorsque Field et ValueName ne sont pas définis, la section entière est verrouillée/chiffrée. Il peut également s'agir d'un des noms réservés suivants :

- `body` : lorsque `Section=response`, cette valeur définit le corps de réponse comme cible. Lorsque `Section=RawRequest`, le corps de demande (s'il existe) est traité.

ValueName
Indique un ou plusieurs noms de valeurs (dans des paires nom-valeur à valeurs multiples comme HTTP_COOKIE) ou les noms des éléments lorsque `Section=urlfield` ou `Section=cookies`.

Invert Valeur `True` ou `False` indiquant s'il est nécessaire d'inverser l'action (à effectuer pour toutes les zones ou ValueNames SAUF celles qui sont spécifiées).

- Lorsque `ValueName` est spécifié, tous les noms sauf ceux indiqués dans `ValueName` sont traités.
- Lorsque `ValueName` n'est pas spécifié, les noms indiqués pour `Field` sont exclus de l'action.

Remarque : Cette action peut être uniquement utilisée avec les actions `Block`, `Encrypt`, et `Replace`. `StartPattern` et `StartPatternRE` ne peuvent pas être utilisées avec une action d'inversement.

StartPattern
Indique le modèle de chaîne de début à rechercher dans les données spécifiées. Les données qui suivent immédiatement le modèle correspondant sont traitées. Si `StartPattern` est utilisé, vous devez également définir `EndPattern` ou Length, à moins de définir Inclusive sur `True`. Lorsque `Inclusive=True`, `StartPattern`, et facultativement `EndPattern`, sont également verrouillés. Cette action est utile lorsque vous souhaitez verrouiller ou chiffrer une chaîne de données constantes.

StartPatternRE
Il s'agit de la version d'expression régulière de StartPattern. Vous pouvez utiliser cette action pour spécifier une expression régulière standard afin de définir le modèle de début à trouver. Vous pouvez utiliser `StartPattern` ou `StartPatternRE`, mais pas les deux.

EndPattern
Représente le modèle de chaîne qui indique la fin des données identifiées par une action StartPattern. Les données jusqu'à `EndPattern` (non inclus) sont traitées (sauf si `Inclusive=True`).

EndPatternRE
Il s'agit de la version d'expression régulière de `EndPattern`. Vous pouvez utiliser cette action pour spécifier une expression régulière standard afin de définir le modèle de fin à trouver. Vous pouvez utiliser `EndPattern` ou `EndPatternRE`, mais pas les deux.

Length Utilisée à la place de `EndPattern` ou de `EndPatternRE`, cette valeur spécifie la taille des données (en octets) à traiter suivant un modèle `StartPattern` (ou `StartPatternRE`).

Inclusive
Valeur `True` ou `False` indiquant si `StartPattern` (ou `StartPatternRE`) et, facultativement, `EndPattern` (ou `EndPatternRE`) sont verrouillés ou chiffrés. La valeur par défaut est `False`.

RepeatCount
Peut être utilisée pour les actions bénéficiant d'une action `StartPattern` ou `StartPatternRE` afin de définir le nombre d'instances de données à traiter correspondant au modèle.

ReplaceString
Représente la chaîne utilisée pour remplacer les données d'origine lorsque `Action=Replace`.

CaseSensitive
Valeur `True` ou `False` indiquant si les recherches de noms de zone et/ou des modèles doivent être sensibles à la casse. La valeur par défaut est `False`. Les recherches sont plus rapides lorsque vous la définissez sur `True`.

StrikeChar
Représente le caractère utilisé pour remplacer les données d'origine verrouillées ou chiffrées. Il peut s'agir de n'importe quel caractère alphanumérique ou symbole, excepté ceux de la liste suivante :

- . (point)
- , (virgule)
- / (barre oblique)
- \ (barre oblique inversée)
- [(crochet gauche)
-] (crochet droit)
- | (barre verticale)
- ' (guillemet simple)
- " (guillemet double)

StrikeLen
Représente la taille facultative (en octets) des données de substitution. Il s'agit du nombre de caractères indiqués dans la zone StrikeChar utilisés pour remplacer les données d'origine (lorsque `Action=Block` ou `Action=Encrypt`).

- Si `StrikeLen` est plus long que les données d'origine, des caractères de substitution supplémentaires sont ajoutés.
- Si `StrikeLen` est plus court que les données d'origine, les caractères contenus dans la zone `StrikeLen` sont remplacés par ceux de la zone `StrikeChar` et les données restantes sont supprimées.
- Si `StrikeLen` contient un nombre négatif, le nombre de caractères représentés par la valeur absolue de `StrikeLen` reste inchangé. Par exemple, pour conserver les quatre derniers caractères ou une valeur, définissez `StrikeLen=-4`.
- Pour plus d'options flexibles, voir BlockingMask.

BlockingMask
Représente une expression régulière spécifiant les caractères des données trouvées à remplacer par le caractère de substitution (ne s'applique pas à l'action Replace). Tous les caractères d'un groupe (défini entre parenthèses) de l'expression régulière sont remplacés par le caractère de substitution. Les caractères correspondant à une partie du modèle situés en dehors d'un groupe ne sont pas remplacés. Exemples :
Le masque suivant verrouille uniquement les chiffres d'un numéro de sécurité social, en laissant apparaître les tirets :

```
BlockingMask=([0-9]{3})-([0-9]{2})-([0-9]{4})
```

Ici, seuls les quatre premiers chiffres d'une carte de crédit sont visibles :

```
BlockingMask=[0-9]{4}([0-9]*)
```

BlockingMask est utilisé à la place de StrikeLen. Vous pouvez utiliser l'une ou l'autre, mais pas les deux.

Remarque : Faites attention lorsque vous utilisez BlockingMask. Si les données ne correspondent pas à l'expression régulière spécifiée pour BlockingMask, elles ne sont ni verrouillées ni chiffrées.

`ReqSetSection`
Définit la section pour la paire nom-valeur d'une action `ReqSet`, `ReqAppend`, ou `ReqDelete`. `ReqSetSection` est obligatoire pour ces trois actions.

`ReqSetField`
Indique le nom d'une paire nom-valeur pour une action `ReqSet`, `ReqAppend`, ou `ReqDelete`. `ReqSetField` est obligatoire pour ces trois actions.

`ReqSetResult`
Cette option est utilisée en association avec `StartPatternRE` afin de produire une valeur formatée pour une action `ReqSet` ou `ReqAppend`. L'expression `StartPatternRE` doit contenir un ou plusieurs "groupes" définis entre parenthèses dans l'expression régulière. `ReqSetResult` représente une chaîne contenant un texte littéral et des paramètres de substitution pour les données capturées par `StartPatternRE`. Exemples :

```
StartPatternRE=name="(.*?)" value="(.*?)"
ReqSetResult=Field
{g1} value: {g2}
```

Le résultat peut être :

```
Field name value: Bob
```

Le premier paramètre de substitution, {g1}, est remplacé par la valeur du premier groupe dans
l'expression régulière. {g2} représente la deuxième valeur, et ainsi de suite. La chaîne de résultat
est ensuite utilisée comme valeur pour l'action `ReqSet` ou `ReqAppend`.

Remarques à propos des actions

- Pour `ReqSet` et `ReqAppend`, il est possible de spécifier la valeur à définir ou à ajouter de deux manières. Vous pouvez utiliser une chaîne littérale en appliquant ReplaceString au texte de votre choix, ou vous pouvez extraire les données de la demande ou de la réponse en utilisant `Section`, `Field`, `ValueName`, `StartPattern`, `StartPatternRE`, `EndPattern` et/ou `EndPatternRE`.
- Lorsque vous utilisez `StartPattern` ou `StartPatternRE` avec l'une de ces actions, le RepeatCount est toujours défini sur 1 (le premier résultat est toujours utilisé).
- `IgnoreSpecial` est toujours défini sur True pour ces actions lorsque `Section` est spécifié. Avec ces actions, aucune manipulation spéciale n'est nécessaire pour les sections `urlfield` ou `cookies`.
- Il est possible d'effacer la valeur d'une zone (paire nom-valeur) sans supprimer la totalité de la zone en utilisant `ReplaceString` sans préciser de valeur :

  ```
  ReplaceString=
  ```
- Tous les retours chariot et les sauts de ligne de la chaîne de valeur sont remplacés par `\r` et `\n`.
- Les modifications des paramètres de confidentialité sont placées en file d'attente et appliquées après la fin de toutes les opérations. Cela signifie que les actions

voient normalement les données d'origine. `ReqSet`, `ReqAppend` et `ReqDelete` assurent le suivi des ajouts, des modifications et des suppressions de zones. Par conséquent, il est possible d'effectuer plusieurs modifications pour une seule zone (par exemple ajouter une zone puis concaténer les données supplémentaires à la valeur) en toute sécurité. L'action Remplacer peut affecter n'importe quel bloc de données de la demande ou de la réponse, c'est pourquoi elle n'est pas incluse dans le suivi des modifications. Pour plus d'efficacité, effectuez les modifications des valeurs de zone à l'aide de `ReqSet` et de `ReqAppend`.

- Lorsque vous utilisez `Field` ou `ValueName` avec `ReqSet` ou `ReqAppend`, vous devez spécifier une zone unique ou un nom de valeur. S'il existe plusieurs noms, la valeur du dernier élément trouvé est utilisée.
- Comme pour la remarque ci-dessus, vous devez éviter de spécifier une seule section pour récupérer la valeur de `ReqSet` ou `ReqAppend`. Cela permet d'obtenir la valeur de la dernière zone (paire nom-valeur) dans la section utilisée pour `ReqSet` ou `ReqAppend`.

Consignation des modifications

La section suivante contient des informations relatives à la consignation des modifications.

Modifications de la confidentialité

Lorsque vous effectuez des modifications dans l'onglet **Règles** concernant le fichier `privacy.cfg`, une version de sauvegarde de l'ancien fichier est enregistrée selon le format suivant : `privacy.cfg.X`, où `X` représente un numéro de version.

- Par défaut, il est possible de conserver à tout moment un maximum de cinq versions.

Consignation des différences

Les modifications des paramètres de confidentialité sont consignées, et les différences de toutes les modifications de la console Web le sont également dans le fichier `conf_changelog.cfg`.

Référence

- Pour des informations générales sur la confidentialité de Tealeaf, voir section "Gestion de la confidentialité des données dans Tealeaf CX" du *Manuel d'installation d'IBM Tealeaf CX*.
- Pour plus d'informations sur la configuration de la confidentialité, voir section "Agent de session de confidentialité" du *Manuel de configuration d'IBM Tealeaf CX*.
  - Tealeaf fournit des filtres de confidentialité préconfigurés que vous pouvez activer et modifier selon les besoins de votre application Web. Voir section "Filtres préconfigurés" du *Manuel de configuration d'IBM Tealeaf CX*.
  - Pour plus d'informations sur la version améliorée de l'agent de session Windows, voir section "Agent de session de confidentialité étendue" du *Manuel de configuration d'IBM Tealeaf CX*.
- Pour plus d'informations sur l'utilitaire de test de la confidentialité, voir section "Utilitaire de test de la confidentialité" du *Manuel de configuration d'IBM Tealeaf CX*.

Statistiques par instance

Lorsque vous sélectionnez une vue qui affiche des statistiques dans plusieurs instances, les données de chacune apparaissent dans une colonne distincte : `ID#0`, `ID#1`, et ainsi de suite.

- Le nombre de colonnes de données affichées correspond au nombre d'instances configurées d'IBM Tealeaf Application de capture passive CX et au nombre d'instances supplémentaires du processus pipelined.

Exemple

Si vous disposez de trois instances de la PCA et cinq instances de pipeline, cinq colonnes sont affichées dans la mesure où l'ensemble constitué des cinq instances de pipeline est le plus volumineux.

- Les trois premières instances contiennent toutes les informations spécifiques des instances de la PCA et de pipeline.
- Les deux dernières instances contiennent uniquement les informations spécifiques aux deux instances restantes de pipeline.

Exemple :
Si vous disposez de six instances de la PCA et trois instances de pipeline, six colonnes sont affichées, dont les trois premières instances uniquement contiennent des informations spécifiques au pipeline dans la mesure où il n'y a que trois pipelines.

Remarque : il est possible de configurer plusieurs instances du processus du pipeline de la PCA dans la build 3403 ou supérieure.

- Pour en savoir plus sur la mesure des performances de chaque pipeline, voir «Section Hits», à la page 149.
- Pour plus d'informations sur la configuration d'instances supplémentaires de pipeline, voir «Console Web de la PCA - Onglet Interface», à la page 71.

Vérification de l'intégrité du système à l'aide de `stats.xml`

Vous pouvez utiliser la sortie `stats.xml` pour contrôler si la PCA reçoit le trafic et s'il est ensuite acheminé vers les destinataires cibles.

Tableau 4. Trafic :

Paramètre	Description et valeur attendue
`<CaptureCurrentFilteredKbytesPerSec>`	Cette valeur indique le nombre de kilooctets par seconde des données filtrées capturées par la PCA. • La valeur doit être positive lorsque la capture fonctionne.

Tableau 4. Trafic : (suite)

Paramètre	Description et valeur attendue
<SslTotalDhCipherConnections>	Cette valeur indique le nombre total de connexions SSL selon le protocole d'échange de clé Diffie-Hellman en cours d'utilisation. **Remarque :** IBM Tealeaf Application de capture passive CX ne prend pas en charge l'utilisation du protocole Diffie-Hellman. Cette valeur doit être de zéro (0).

Tableau 5. Distribution :

Paramètre	Description et valeur attendue
<StateText>	Cette valeur indique l'état de la connexion entre la PCA et le serveur Windows cible. • Elle doit indiquer connected.
<TotalHitsQueued>	Nombre total de hits en attente de distribution pour le serveur IBM Tealeaf CX. • Cette valeur doit être égale à <TotalHitsDelivered>.

Pour plus d'informations sur les options disponibles pour ctcstats, exécutez ce qui suit sur la ligne de commande en tant qu'utilisateur `ctccap` :

```
./ctcstats -h
```

Processus du logiciel de capture

Pour plus d'informations concernant les processus de la PCA, voir Chapitre 1, «Présentation de Passive Capture», à la page 1.

Statistiques de Passive Capture

Les sections suivantes fournissent une description des définitions de statistiques de Passive Capture.

Légende

- XML : noeud XML dans `stats.xml`
- Ecran de console : valeur d'affichage dans l'onglet Statistiques de la console Web de la PCA
  - Dans cette colonne, la valeur `not available` indique que la statistique n'est pas rapportée par défaut dans la console Web de la PCA.
- Description : texte décrivant la statistique.

Section Général

Tableau 6. Section Général

XML	Ecran de console	Description
<CaptureVersion>	Capture version	Numéro de version du logiciel Passive Capture.

Tableau 6. Section Général (suite)

XML	Ecran de console	Description
<CapturedPctCpu>	Captured CPU usage percent (high)	Utilisation de l'UC actuelle pour le processus.
<CoreDumpCount>	Number of coredumps	Nombre d'images-mémoire produites par les processus de la PCA. Il s'agit d'un nombre de fichiers d'images-mémoire du sous-répertoire /usr/local/ctccap.
<CpuLoadPct>	CPU load percentage	Pourcentage total de la charge de l'UC rapporté par le système.
<InstanceCount>	Number of instances	Nombre d'instances en cours d'exécution (paires listend et reassd).
<PeerCount>	Number of delivery peers	Nombre de connexions socket envoyées par Deliverd aux serveurs de traitement Tealeaf.
<ProcessCount>	Number of processes	Nombre total de processus du logiciel Passive Capture, de processus du serveur Apache et ainsi de suite.
<ProcessClassCount	Number of process classes	Nombre total de processus spécifiques de Tealeaf regroupés en classes.
<ReassdPctCpu>	Reassd CPU usage percent (high)	Pourcentage d'utilisation du processeur le plus élevé rapporté par le système dans tous les processus Reassd. Il peut y avoir plusieurs processus Reassd, mais généralement il n'y en a qu'un.

Section Temps

Tableau 7. Section temps

XML	Ecran de console	Description
<LastReset>	Last time statistics were reset	Heure et date de suppression des statistiques.
<LastResetSecondsUtc>	Last time statistics were reset in UTC seconds	Secondes en temps UTC écoulées depuis la dernière suppression des statistiques.
<LastResetUtc>	Last time statistics were reset in UTC	Heure et date de suppression des statistiques au Temps Universel Coordonné.
<LastRestart>	Last time capture entered main loop	Heure et date auxquelles le processus captured a redémarré ses processus enfants.

Tableau 7. Section temps (suite)

XML	Ecran de console	Description
<LastRestartSecondsUtc>	`Last time capture entered main loop in UTC seconds`	Secondes en temps UTC écoulées depuis que le processus captured a redémarré ses processus enfants.
<LastRestartUtc>	`Last time capture entered main loop in UTC`	Heure et date en temps UTC auxquelles le processus captured a redémarré ses processus enfants.
<LocalTime>	`Local time`	Heure locale du système
<LocalTimeSecondsUtc>	`Local time in UTC seconds`	Heure locale du système en secondes UTC
<LocalTimeUtc>	`Local time in UTC`	Heure locale du système au Temps Universel Coordonné
<NumSystemRestarts>	`Number of times capture entered main loop`	Nombre total de redémarrages des processus enfants de captured depuis le démarrage du logiciel Passive Capture.
<TimeCpuUptime>	`Time since last OS reboot (days, hours, minutes, seconds)`	Temps écoulé depuis le redémarrage du système d'exploitation.
<TimeCpuUptimeSeconds>	`Seconds since last OS reboot`	Secondes écoulées depuis le dernier redémarrage du système d'exploitation.

Section Mémoire

Les statistiques relatives à la mémoire suivantes sont toutes liées et effectuent un suivi des unes et des autres.

Tableau 8. Section Mémoire

XML	Ecran de console	Description
<MemoryListendSize>	`Listend size`	Encombrement de mémoire actuel du processus comme indiqué par le système d'exploitation, en octets. Généralement cette valeur doit être inférieure à 20 Mo.

Tableau 8. Section Mémoire (suite)

XML	Ecran de console	Description
<MemoryListendMaxSize>	`Listend max size`	Taille maximale (en octets) de l'encombrement de mémoire du processus comme indiqué par le système d'exploitation. Cette valeur change en fonction de différentes exigences internes. Généralement, elle suit la taille actuelle avec une marge d'erreur faible et indique sa cote maximale atteinte.
<MemoryListendMemoryIn_use>	`Listend memory in use`	Taille (en octets) de la mémoire du processus utilisée, par rapport à la mémoire nécessaire allouée de manière dynamique. Cette valeur augmente en fonction de ses besoins, jusqu'à 100 Mo pour les mémoires tampon des paquets internes.
<MemoryListendMaxMemoryIn_use>	`Listend max memory in use`	Indicateur de cote maximale atteinte pour la valeur en cours d'exécution ci-dessus.
<MemoryReassdSize>	`Reassd size`	Volume (en octets) de l'encombrement de mémoire actuel du processus comme indiqué par le système d'exploitation. Cette valeur indique la mémoire en cours qui lui est allouée, y compris son encombrement. Le volume peut varier de quelques mégaoctets à 1 Go ou plus.
<MemoryReassdMaxSize>	`Reassd max size`	Cote maximale atteinte pour le volume de la mémoire actuel ci-dessus.

Tableau 8. Section Mémoire (suite)

XML	Ecran de console	Description
<MemoryReassdMemoryIn_use>	Reassd memory in use	Quantité de mémoire du processus utilisée basée sur ses demandes d'allocation de mémoire dynamique. Cette valeur peut également varier de quelques mégaoctets à plus d'1 Go selon ses exigences en matière de traitement de l'activité du trafic réseau en cours. Il n'y a pas de valeur particulière, mais elle est généralement inférieure à 500 Mo.
<MemoryReassdMaxMemoryIn_use>	Reassd max memory in use	Cote maximale atteinte pour la quantité de mémoire en cours ci-dessus.
<MemoryListendOutputBuffers>	Listend output buffers	Mémoire Current utilisée dans la mémoire tampon de sortie (en octets) pour le trafic de paquets filtré du processus listend. Ce tampon mémoire sert à mettre en mémoire tampon le trafic circulant de listend vers reassd via son canal de communication. La processus reassd extrait les paquets du trafic pour les traiter. La taille par défaut de cette mémoire tampon est de 100 Mo.
<MemoryListendOutputBuffersMax>	Listend output buffers max	Cote maximale atteinte pour la taille de la mémoire en cours ci-dessus.
<MemoryDeliveryQueue>	Delivery queue	Taille (en octets) de la mémoire tampon de distribution des hits Current pour envoyer les hits via le socket du serveur d'IBM Tealeaf CX.
<MemoryDeliveryQueueMax>	Delivery queue max	Cote maximale atteinte pour la valeur de la taille de la file d'attente ci-dessus.

Tableau 8. Section Mémoire (suite)

XML	Ecran de console	Description
<MemorySslSessionCacheEntries>	`SSL session cache entries`	Nombre d'entrées de session SSL en cours stockées dans la table de mémoire cache. Le paramètre de configuration conf détermine le nombre d'entrées pouvant être stockées à la fois (10 000 en général). • Pour plus d'informations sur le réglage du paramètre de la limite maximale, voir la statistique SSL `Total session cache misses` ci-dessous.
<CpuUsagePctHigh>	indisponible	Pourcentage d'utilisation du processeur (élevé)
<CpuUsagePctTotal>	indisponible	Pourcentage d'utilisation du processeur (total)
<Id>	indisponible	ID de processus dans le cadre des processus de la PCA
<MemUsagePctHigh>	indisponible	Pourcentage d'utilisation de la mémoire (élevé)
<MemUsagePctTotal>	indisponible	Pourcentage d'utilisation de la mémoire (total)
<Name>	indisponible	nom du processus
<ProcessCount>	indisponible	Nombre de processus
<VirtualMemorySizeKbytesHigh>	indisponible	Taille de la mémoire virtuelle (en kilooctets) élevée
<VirtualMemorySizeKbytesTotal>	indisponible	Taille de la mémoire virtuelle (en kilooctets) totale

Section TCP

Tableau 9. Section TCP

XML	Ecran de console	Description
<TcpTotalPacketsRcvd>	`Total packets rcvd`	Nombre de paquets TCP reçus par le réassembleur TCP.
<TcpTotalPacketsRcvdPerSec>	`Total packets rcvd per second`	Débit de paquets TCP reçus par seconde
<TcpTotalConnections>	`Total connections`	Nombre de nouvelles connexions TCP créées par le réassembleur TCP
<TcpTotalConnectionsPerSec>	`Total connections per second`	Débit de nouvelles connexions TCP créées par seconde
<TcpTotalClosedConnections>	`Total closed connections`	Nombre de connexions TCP fermées par le réassembleur TCP
<TcpTotalRstConnections>	`Total reset connections`	Nombre de connexions TCP réinitialisées. Si le nombre est important, cela peut indiquer un problème de connexion.

Tableau 9. Section TCP (suite)

XML	Ecran de console	Description
<TcpSyn_waitConnections>	SYN/WAIT connections	Nombre Current de connexions TCP recevant uniquement le premier paquet d'établissement de liaison de synchronisation. Ce nombre doit coïncider avec la valeur "connexions Current", inférieure à 50 pour cent, selon l'activité du trafic réseau. Si cette valeur dépasse largement ce pourcentage, cela peut indiquer un problème lié au trafic du port miroir.
<TcpSyn_waitConnectionsMax>	SYN/WAIT connections max	Cote maximale atteinte pour la valeur ci-dessus.
<TcpTotalSyn_waitConnectionsAged>	Total SYN/WAIT connections aged	Affiche le nombre de connexions SYN/WAIT supprimées en raison de leur ancienneté.
<TcpTotalSyn_waitConnectionsDestroyed>	Total SYN/WAIT connections destroyed	Nombre de connexions SYN/WAIT détruites lorsque la limite maximale est atteinte, afin de libérer de l'espace pour la création de nouvelles connexions. Si ce nombre augmente rapidement sur une courte période (5 minutes), il est possible que les limites maximales par défaut soient trop basses par rapport au volume du trafic réseau capturé. Indiquez une valeur plus élevée pour réduire les pertes. Cela peut également indiquer un problème lié à l'infrastructure réseau qui ne fournit pas un trafic réseau complet.
<TcpTotalOutsyncSyn_waitConnections>	Total out-of-sync SYN/WAIT connections	Nombre total de connexions où les paquets de l'établissement de liaison de synchronisation, SYN1 et SYN2, sont inversés. Le client reçoit le paquet SYN du serveur avant réception du paquet SYN du serveur par le client.
<TcpCurrentConnections>	Current connections	Nombre Current de connexions d'établissement de liaison de synchronisation effectuées (connexions établies).
<TcpCurrentConnectionsMax>	Current connections max	Cote maximale atteinte pour la valeur ci-dessus.
<TcpTotalCurrentConnectionsAged>	Total Current connections aged	Affiche le nombre de connexions en cours supprimées en raison de leur ancienneté.
<TcpTotalCurrentConnectionsDestroyed>	Total Current connections destroyed	Nombre de connexions détruites lorsque la limite maximale est atteinte. Cela se produit afin de libérer de l'espace pour la création de nouvelles connexions. Si ce nombre augmente rapidement sur une courte période (5 minutes), il est possible que les limites maximales par défaut soient trop basses par rapport au volume du trafic réseau capturé. Indiquez une valeur plus élevée pour réduire les pertes. Cela peut également indiquer un problème lié à l'infrastructure réseau qui ne fournit pas un trafic réseau complet.
<TcpTotalConnectionsReaped>	Total Connections reaped	Connexions par seconde ne pouvant pas être déchiffrées en raison d'une clé manquante
<TcpTime_waitConnections>	TIME_WAIT connections	Nombre Current de connexions, dont l'état est fermé/en attente mais pas fermé, ayant reçu les paquets FIN.
<TcpTime_waitConnectionsMax>	TIME_WAIT connections max	Cote maximale atteinte pour la valeur ci-dessus.
<TcpTotalOooConnectionsDeleted>	Total out-of-order connections deleted	Indique le nombre de connexions défectueuses supprimées. La valeur de cette statistique se réinitialise automatiquement lorsqu'elle dépasse 5 000 000.
<TcpTotalOooConnections>	Total out-of-order connections	Indique le nombre de connexions par paquet défectueuses. Si ce nombre est élevé ou s'approche du nombre total de connexions, l'infrastructure réseau qui fournit le trafic aux ports de capture ne peut pas être nettoyée et certains hits ne peuvent pas être correctement réassemblés car une réorganisation trop importante des paquets est requise. Il est possible que le processeur soit fortement sollicité pour le processus de capture.
<TcpTotalRolloverConnections>	Total rollover connections	Nombre total de connexions pour lesquelles le numéro de séquence TCP est passé à 0
<TcpTotalMissingPktConnections>	Total missing packet connections	Nombre total de connexions pour lesquelles il manque des paquets
<TcpCurrentStreamingConnections>	Current streaming connections	Ni exécuté ni utilisé
<TcpTotalStreamingConnections>	Total streaming connections	Ni exécuté ni utilisé
<TcpTotalAckedButUnseenPackets>	Total ACKed but unseen packets	Nombre de paquets TCP ACK reçus sans paquet de données TCP correspondant ayant accusé réception de la connexion TCP.

Tableau 9. Section TCP (suite)

XML	Ecran de console	Description
<TcpTotalAckRollbacks>	Total ACK rollbacks	Nombre de numéros de séquence de paquets ACK inférieurs à ceux attendus dans le réassembleur TCP.
<TcpAlienPacketsRcvd>	Alien packets rcvd	Nombre de paquets TCP ne correspondant à aucune connexion TCP da la table du réassembleur TCP des connexions connues en cours. Il est nécessaire de comparer le nombre de paquets étrangers à la valeur `Total packets captured`. Le pourcentage devrait être de moins de 10 pour cent.
<TcpTotalChecksumErrors>	Total checksum errors	Nombre d'erreurs de total de contrôle des paquets TCP incorrects. Si des erreurs sont signalées, votre infrastructure réseau effectue la mise en miroir du trafic pour la machine hôte de Passive Capture avec des valeurs incorrectes de total de contrôle des paquets. **Remarque :** si vous rencontrez un grand nombre d'erreurs de total de contrôle, il se peut que le problème soit lié à plusieurs facteurs, par exemple le déchargement du total de contrôle effectué au niveau de la carte d'interface réseau. Contactez votre service informatique afin d'identifier si cette fonction est activée et, le cas échéant, la désactiver, puis revérifiez la valeur de cette statistique.
<TcpErrors>	Errors	Ni exécuté ni utilisé.
<TcpErrorsperSec>	TCP Errors per Second	Ni exécuté ni utilisé.
<TcpTotalDuplicatePackets>	Total back-to-back duplicate packets	Indique le nombre de paquets dupliqués qui se suivent dans le trafic de capture filtré. S'ils sont nombreux, les ports miroir du commutateur réseau ne sont pas correctement configurés et dupliquent le trafic. Dans ce cas, la statistique correspond environ à la moitié de la valeur indiquée pour `Total packets rcvd`. Bien que les processus de capture soient en mesure gérer les paquets du trafic dupliqué, ils sont inutiles et affectent les performances du système lorsqu'elles sont déjà proches du niveau maximal. La bande passante des cartes d'interface réseau pour la capture est également utilisée inutilement. • Voir «Comment la PCA gère-t-elle la duplication des paquets TCP ?», à la page 282.

Section SSL

Tableau 10. Section SSL

XML	Ecran de console	Description
<SslTotalTIs11Sessions>	Total TLS1.1 sessions	Nombre total de sessions SSL utilisant le protocole TLS1.1.
<SslTotalTIs11SessionsDecrypted>	Total TLS1.1 sessions decrypted	Nombre total de sessions SSL utilisant le protocole TLS1.1 et déchiffrées correctement.
SslTotalTls12Sessions	Total TLS1.2 sessions	Nombre total de sessions SSL utilisant le protocole TLS1.2.
SslTotalTls12SessionsDecrypted	Total TLS1.2 sessions decrypted	Nombre total de sessions SSL utilisant le protocole TLS2.1 et déchiffrées correctement.
<SslTotalNewHandshakes>	Total new handshakes	Nombre de nouvelles sessions d'établissement de liaison SSL produites. "New" indique que la session SSL n'a pas été trouvée dans la table de mémoire cache de la session SSL.

Tableau 10. Section SSL (suite)

XML	Ecran de console	Description
<SslTotalResumedHandshakes>	Total resumed handshakes	Indique un total cumulatif des établissements de liaison SSL repris produits. Cette statistique montre à quel point les sites Web tirent parti des performances de la connexion SSL. Si le nombre est zéro, cela signifie que de nouveaux établissements de liaison SSL en forte surcharge sont traités sur des sites présentant des problèmes de performances.
<SslRecordsRcvd>	Records rcvd	Nombre d'enregistrements SSL capturés pouvant copier plusieurs paquets.
<SslTotalHandshakes>	Total handshakes	Nombre de sessions d'établissement de liaison SSL correctement négociées. Ce nombre indique que le déchiffrement du trafic SSL a fonctionné.
<SslHangingConnections>	Hanging connections	Ni exécuté ni utilisé.
<SslCurrentConnections>	Current connections	Ni exécuté ni utilisé.
<SslHitCount>	Hit Count	Ni exécuté ni utilisé.
<SslCurrentHitsPerSec>	Current hits per second	Cette statistique est un indicateur important des performances et de la disponibilité du système. Elle affiche le nombre actuel du débit de hits SSL par seconde générés par les processus de capture. Environ 150 hits issus des nouveaux établissements de liaison SSL sont attendus, sans recourir à l'accélération matérielle SSL. Le déchiffrement SSL est une opération qui sollicite beaucoup le processeur et le système de capture. Ces statistiques sont mises à jour toutes les 5 secondes.
<SslMaxHitsPerSec>	Maximum hits per second	Affiche le débit maximum de hits SSL par seconde générés par les processus de capture.
<SslAvgHitsPerSec>	Average hits per second	Indique une moyenne cumulative du nombre de hits SSL par seconde traités. Cette statistique donne un aperçu global des opérations SSL sur une longue période d'exécution au lieu d'une courte période.
<SslNewHandshakesPerSec>	New handshake hits per second	Fournit un aperçu du débit des nouveaux établissements de liaison SSL qui se produisent.
<SslNewHandshakesPerSecMax>	Maximum new handshake hits per second	Débit maximal des nouveaux établissements de liaison SSL par seconde.
<SslResumedHandshakesPerSec>	Resumed handshake hits per second	Débit maximal des établissements de liaison SSL repris par seconde
<SslResumedHandshakesPerSecMax>	Maximum resumed handshake hits per second	Débit maximal des établissements de liaison SSL repris par seconde

Tableau 10. Section SSL (suite)

XML	Ecran de console	Description
`<SslConnectionDataLen>`	`Connection data length`	Taille moyenne des données (en octets) d'une connexion SSL sur une période de 5 secondes (échantillonnage). Cette statistique est utilisée pour calculer la taille moyenne d'un hit SSL.
`<SslHitDataLen>`	`Hit data length`	Valeur calculée pour la taille moyenne (en octets) des données d'un hit SSL.
`<SslTotalNewSessionTicketSessions>`	`Total new SessionTicket sessions`	Cette valeur indique le nombre de nouvelles sessions SSL en utilisant l'extension de tickets de session TLS. Pour que le comptage soit valable, le client et le serveur doivent prendre en charge l'extension. Par exemple, si le client envoie une demande en utilisant l'extension de tickets de session et que le serveur la rejette car il ne la prend pas en charge, la session n'est pas prise en compte.
`<SslTotalResumedSessionTicketSessions>`	`Total resumed SessionTicket sessions`	Cette valeur correspond au nombre de sessions contenant des tickets de session TLS reprises après avoir été interrompues.
`<SslTotalDecryptedSessionTicketSessions>`	`Total decrypted SessionTicket sessions`	Cette valeur représente le nombre de nouvelles sessions SSL et de sessions SSL reprises déchiffrées par la PCA.
`<SslTotalSessionTicketSessionCacheMisses>`	`Total SessionTicket session cache misses`	Cette valeur correspond au nombre de sessions SSL reprises que la PCA n'a pas été en mesure de déchiffrer, généralement lorsqu'elle n'a pas vu la nouvelle session SSL d'origine.
`<SslTotalEphemeralRsaConnections>`	`Total ephemeral RSA connections`	Affiche le nombre de connexions SSL ayant utilisé des chiffrements "transitoires", par exemple le faible chiffrement RSA de 40 bits. Ils sont généralement utilisés par les navigateurs internationaux n'étant pas autorisés à utiliser un chiffrement renforcé de 128 bits. **Remarque :** les algorithmes indéchiffrables ne peuvent pas être déchiffrés ultérieurement. Un message provenant du journal d'erreurs est également généré pour fournir les informations sur l'IP du client.

Tableau 10. Section SSL (suite)

XML	Ecran de console	Description
<SslTotalDhCipherConnections>	Total Diffie-Hellman cipher connections	Calcule le nombre de connexions SSL utilisant le protocole de chiffrement Diffie-Hellman. • Cette méthode éphémère ne peut pas être déchiffrée ultérieurement. Seul le serveur Web peut la lancer et non le navigateur client. Si la valeur est différente de zéro, cela signifie qu'un ou plusieurs serveurs Web a configuré ses préférences de suite de chiffrement pour utiliser cette méthode en particulier. • Pour activer le déchiffrement ultérieur, le serveur Web doit modifier ses préférences pour le chiffrement SSL afin de supprimer cette méthode et de la remplacer par une autre, par exemple les méthodes de chiffrement 256 bits AES et RSA.
<SslTotalNullCipherConnections>	Total Null Cipher Connections	Nombre de connexions SSL ne contenant aucune méthode de chiffrement.
<SslTotalHsmKeysLoaded>	Total HSM keys loaded	Indique le nombre de clés SSL chargées par la PCA au démarrage à partir du magasin de clés Sun HSM pour chaque instance de la PCA.
<SslMissingKeys>	Missing keys	Nombre de clés SSL utilisées auxquelles aucun fichier PEM de clé SSL ne correspondait.
<SslMissingKeysPerSec>	Missing keys per second	Connexions par seconde ne pouvant pas être déchiffrées en raison d'une clé manquante.
<SslTotalBadHandshakeSeqErrors>	Total Bad Handshake Sequence Errors	Ni exécuté ni utilisé.
<SslTotalUnknownCipherErrors>	Total Unknown Cipher Errors	Ni exécuté ni utilisé.
<SslErrors>	Errors	Ni exécuté ni utilisé.
<SslTotalSessionCacheMisses>	Total session cache misses	Lorsqu'un enregistrement de session SSL est reçu pour être déchiffré, une vérification est effectuée pour voir si le cache contient les informations de l'algorithme de déchiffrement pour cette session. S'il ne les contient pas, l'enregistrement est considéré comme un échec en mémoire cache. Dans la mesure où il s'agit d'un enregistrement, il est supposé que la liaison SSL a été établie et que le cache contient sûrement les informations de son algorithme de chiffrement. Cela peut se produire lorsque Passive Capture a été redémarré et que le programme commence la capture de sessions SSL en cours, ou qu'il a dépassé la limite par défaut du nombre d'entrées de cache simultanées fixée à 10 000 et que les entrées LRU ont été supprimées.

Tableau 10. Section SSL (suite)

XML	Ecran de console	Description
`<SslSessionCacheMissesPerSec>`	`Session cache misses per second`	Débit d'échecs en mémoire cache de session par seconde.
`<SslOldestSessionCacheEntry>`	`Oldest session cache entry`	Indique (en minutes) l'entrée de cache SSL la plus ancienne. Cette statistique permet d'estimer s'il existe suffisamment d'entrées de cache pour ajuster sa table afin de gérer un site volumineux tout en ayant un faible impact sur la performance.
`SslHitCount>`	`SSL hit count`	Nombre de hits SSL
`<SslTotalCaptureType1>`	`SSL Total Capture Type 1`	Permet de compter les hits SSL du type de capture 1 (pages).
`<SslPageViewPct>`	`Percent of ssl page views to page views`	Pourcentage de pages affichées protégées par SSL

Section Hits

Tableau 11. Section Hits

XML	Ecran de console	Description
`<HitsCaptured>`	`Captured`	Nombre de hits pour lesquels l'analyseur HTTP a été en mesure de former un hit de demande et de réponse complet.
`<HitsCapturedPerSec>`	`Captured before hit processing per second`	Indique le débit actuel des hits capturés (voir ci-dessus). Cette statistique donne un aperçu du nombre de hits avant qu'ils ne soient traités, rejetés, etc.
`<HitsRejectedResponse>`	`Rejected response`	Ni exécuté ni utilisé.
`<HitsRejectedResponseBody>`	`Rejected response body`	Ni exécuté ni utilisé.
`<HitsRejectedHits>`	`Rejected hits`	Dans Tealeaf, en mode de capture BusinessIT, représente le nombre de hits dont la réponse a été rejetée lorsque leur extension URL figure dans la liste des extensions exclues. Le hit est quand même formé et distribué mais la réponse est manquante, par exemple seule la demande est enregistrée. Exemples d'extensions URL exclues : GIF, BMP, CSS, JS, etc.
`<HitsUndeliveredHitsWhilePassive>`	`Undelivered hits while passive`	Affiche les hits supprimés lorsque Passive Capture joue le rôle d'un noeud passif.
`<HitsCurrentNonSslHitsPerSec>`	`Current non-SSL hits per second`	Indique les débits actuels des hits non-SSL par seconde en cours de traitement. Cette statistique donne un aperçu du nombre de hits non-SSL traités étant déchiffrés par Passive Capture. Il est possible que le trafic SSL de certains sites s'arrête avant que Passive Capture ne le reçoive.

Tableau 11. Section Hits (suite)

XML	Ecran de console	Description
`<HitsMaxNonSslHitsPerSec>`	`Maximum non-SSL hits per second`	Indique les débits maximaux des hits non-SSL par seconde en cours de traitement. Cette statistique donne un aperçu du nombre de hits non-SSL traités étant déchiffrés par Passive Capture. Il est possible que le trafic SSL de certains sites s'arrête avant que Passive Capture ne le reçoive.
`<HitsAvgNonSslHitsPerSec>`	`Average non-SSL hits per second`	Indique les débits moyens des hits non-SSL par seconde en cours de traitement. Cette statistique donne un aperçu du nombre de hits non-SSL traités étant déchiffrés par Passive Capture. Il est possible que le trafic SSL de certains sites s'arrête avant que Passive Capture ne le reçoive.
`<HitsCurrentToDeliveryHitspersec>`	`Current to delivery hits per second`	Indique les débits actuels des hits envoyés vers le système de distribution de Passive Capture. Il est possible que le système de distribution soit surchargé en raison de différents problèmes de connexion réseau. Par exemple si la bande passante de la carte d'interface réseau est saturée, des hits peuvent être supprimés.
`<HitsMaxToDeliveryHitspersec>`	`Maximum to delivery hits per second`	Indique les débits maximaux des hits envoyés vers le système de distribution de Passive Capture. Il est possible que le système de distribution soit surchargé en raison de différents problèmes de connexion réseau. Par exemple si la bande passante de la carte d'interface réseau est saturée, des hits peuvent être supprimés.
`<HitsTotalCaptureType1>`	`Total Capture Type 1 Hits`	Nombre de hits de Type de capture 1 ayant été capturés.
`<HitsTotalCaptureType2>`	`Total Capture Type 2 Hits`	Nombre de hits de Type de capture 2 ayant été capturés.
`<HitsTotalCaptureType3>`	`Total Capture Type 3 Hits`	Nombre de hits de Type de capture 3 ayant été capturés.
`<HitsTotalCaptureTypeOther>`	`Total Capture Type Other Hits`	Nombre de hits d'un type de capture non identifié ayant été capturés.
`<HitsTotalLargeHits>`	`Total Hits Identified as Too Large`	Nombre de hits identifiés trop volumineux pour être capturés.
`<HitsTotalStreamingHits>`	`Total Streaming Hits`	Nombre total de hits diffusés en flux ayant été capturés.
`<HitsTotalNonHttpTypeErrors>`	`Total non-Http type errors`	Calcule le nombre de hits dont la chaîne du protocole HTTP ne figure pas dans l'en-tête. Dans ce cas, le hit est supprimé.

Tableau 11. Section Hits (suite)

XML	Ecran de console	Description
<HitsTotalBogusHttpErrors>	Total invalid HTTP errors	Calcule le nombre de hits ne suivant pas de règles de format de protocole HTTP spécifiques concernant les en-têtes, par exemple les caractères d'en-tête manquants, les caractères superflus de retour chariot ou de saut de ligne, etc.Dans ce cas, le hit est supprimé.
<HitsTotalClientSpeaksFirstErrors>	Total responses before requests errors	Indique qu'un hit HTTP a été réassemblé avec une réponse avant une demande.
<HitsTotalMoreRespThanReqErrors>	Total more responses than requests errors	Indique, dans une connexion TCP, où se forment plusieurs hits, qu'il existe plus de réponses que de demandes. Cela signifie que le nombre de demandes était insuffisant pour correspondre aux réponses des hits. Tous les hits suivants sont supprimés une fois que cette condition est reconnue dans la connexion TCP.
<HitsTotalUnansweredReqErrors>	Total unanswered requests errors	Indique, dans une connexion TCP, que pour plusieurs hits des réponses sont manquantes par rapport au nombre de demandes.
<HitsTotalUnfinishedReqErrors>	Total unfinished request errors	Nombre total de demandes HTTP terminées avant que leur taille ne soit indiquée. Ces erreurs peuvent survenir lorsque l'en-tête de requête indiquant la taille du contenu n'a pas correctement été calculée pour le corps de demande réel. Par exemple, lorsque la taille indiquée est supérieure à la valeur réelle des données. **Remarque :** cette statistique est disponible dans PCA Build 3500 ou supérieure.
<HitsTotalUnfinishedRespErrors>	Total unfinished response errors	Nombre total de réponses HTTP terminées avant que leur taille ne soit indiquée. Ces erreurs peuvent survenir lorsque l'en-tête de réponse pour la longueur du contenu n'a pas correctement été calculé pour les données de réponse réelles. Par exemple, lorsque la longueur précisée est supérieure à la valeur réelle des données.
<HitsTotalRespTimerExpiredErrors>	Total response timer expired errors	Indique, dans une connexion TCP, qu'aucune réponse n'a été renvoyée après une requête lancée selon le délai d'attente spécifié dans les paramètres de la transmission TCP. La valeur par défaut est 120 secondes.

Tableau 11. Section Hits (suite)

XML	Ecran de console	Description
<HitsTotalXmitTimerExpiredErrors>	Total packet transmission timer expired errors	Indique, dans une connexion TCP, que les paquets doivent arriver dans le délai d'attente défini dans les paramètres de la transmission TCP. La valeur par défaut est 120 secondes.
<HitsTotalTlapiReparseRespNullErrors>	Total TLAPI invalid response errors	Calcule le nombre de hits dans TLapi ne contenant aucune réponse.
<HitsTotalTlapiReqStartExtraBytes>	Total TLAPI request start extra bytes	Indique les hits dans TLapi possédant des caractères de retour chariot, de saut de ligne ou null au début de la demande. Il s'agit uniquement du nombre de conditions d'avertissement. Même si cela ne correspond pas, les caractères superflus sont ignorés et la vérification continue si le reste de la demande est valide.
<HitsTotalTlapiInvalidReqErrors>	Total TLAPI invalid request errors	Calcule le nombre de hits dans TLapi ne contenant aucune demande. Dans ce cas, le hit est supprimé.
<HitsTotalTlapiReqCorruptErrors>	Total TLAPI request corrupt errors	Calcule le nombre de hits dans TLapi lorsque la demande se termine de manière inattendue. Généralement, certains caractères superflus sont filtrés, ce qui ne laisse rien pour la formation d'une demande. Il en est de même lorsqu'après une méthode de demande (GET, POST, etc.) rien ne suit dans la ligne. Dans ce cas, le hit est supprimé.
<HitsTotalTlapiReparseRespCorruptErrors>	Total TLAPI response corrupt errors	Calcule le nombre de hits dans TLapi ne contenant aucune réponse. Cela peut se produire lorsqu'une connexion TCP se ferme de manière inattendue avant la capture d'une réponse de hit. Le hit incomplet est quand même envoyé vers TLapi pour confirmer l'existence d'un hit complet ou non.
<HitsTotalInflateRequestCandidates>	Total candidates for inflate request	Nombre total de hits dont le corps de demande compressé (données POST) a subi une tentative de décompression.
<HitsTotalInflateRequestsCompleted>	Total requests inflated	Nombre total de hits pour lesquels le corps de demande compressé a été décompressé avec succès.
<HitsTotalInflateRequestsFailed>	Total failed attempts to inflate the request	Nombre total de hits pour lesquels la décompression du corps de demande a échoué.
<HitsTotalInflateResponseCandidates>	Total candidates for inflate response	Nombre total de hits dont la réponse compressée a subi une tentative de décompression.
<HitsTotalInflateResponsesCompleted>	Total responses inflated	Nombre total de hits pour lesquels la réponse a été décompressée avec succès.

Tableau 11. Section Hits (suite)

XML	Ecran de console	Description
<HitsTotalInflateResponsesFailed>	Total failed attempts to inflate the response	Nombre total de hits dont la décompression de la réponse a échoué.
<HitsTotalDeflateResponseCandidates	Total candidates for deflate response	Nombre total de candidats pour la réponse dont le mécanisme de compression est deflate
<HitsTotalDeflateResponsesCompleted>	Total responses deflated	Total des réponses compressées
<HitsTotalDeflateResponsesFailed>	Total failed attempts to deflate the response	Nombre de tentatives de compression de la réponse échouées
<HitsTotalDroppedBusinessModeExtension>	Total dropped due to business mode and extension	Nombre de hits abandonnés lorsque le mode Business et l'extension sont activés
<HitsTotalDroppedBusinessModeResponse>	Total dropped due to business mode and response	Nombre de hits abandonnés lorsque le mode Business et la réponse sont activés
<HitsTotalDroppedByDelimagesFeature>	Nombre de hits abandonnés lorsque le mode businessIT et le jeu de fonctions DelImages sont activés	Nombre de hits d'image, correspondant à des critères spécifiques, abandonnés lorsque DelImages est activé dans la PCA • Voir «Console Web de la PCA - Onglet Pipeline», à la page 101.
<HitsTotalDroppedInvalidMethod>	Total dropped due to invalid HTTP method	Nombre de hits abandonnés en raison d'une méthode HTTP non valide
<HitsTotalDroppedByParseRequest>	Total dropped due to HTTP request parsing error	Nombre de hits abandonnés par la fonction parserequest
<HitsTotalDroppedByParseResponse>	Total dropped due to HTTP response parsing errors	Nombre de hits abandonnés par la fonction d'analyse de la réponse
<HitsTotalDroppedByPrivacy>	Total dropped by privacy rules	Nombre de hits abandonnés par les règles de confidentialité
<HitsTotalDroppedBySampling>	Total dropped by sampling	Nombre de hits abandonnés par la fonction de test

Tableau 11. Section Hits (suite)

XML	Ecran de console	Description
<HitsTotalDroppedHitArrivedTooLate>	Total dropped because hit arrived too late	Nombre de hits abandonnés lorsqu'ils ont dépassé le délai d'attente • Si, lorsque la totalité du hit est envoyée vers le pipeline de la PCA, la différence entre l'horodatage du premier paquet de demandes et l'horodatage d'arrivée est de plus d'une heure, le hit est marqué comme "en retard" pour un traitement normal. Ces hits sont abandonnés pour la suite du traitement par la PCA. – Cette limite d'une heure est codée en dur et n'est pas modifiable. – Tous les hits entrant dans le pipeline de la PCA possèdent un horodatage d'arrivée (TLapiArrivalTimeEx) inséré dans l'enregistrement de la demande dans la section [timestamp]. • Les retards au niveau du pipeline de la PCA peuvent être dus à différents problèmes se produisant le plus souvent en dehors de la PCA.
<HitsTotalDroppedMaxDataSize>	Total dropped because hit exceeds max data size	Nombre de hits abandonnés lorsque la taille maximale est dépassée
<HitsTotalDroppedReqHeaderExceedsMaxReqSize>	Total dropped due to HTTP request hdr too large	Nombre de hits abandonnés lorsque la taille maximale de l'en-tête de requête est dépassée
<HitsTotalDroppedTcldHitError>	Total dropped tcld hits error	Nombre de hits abandonnés pour le processus tcld en cas d'erreurs **Remarque :** cet élément est disponible dans PCA Build 3403 ou supérieure.
<HitsAssembledHitsProcessedPerSecAvg>	Average assembled hits processed per second	Nombre moyen de hits traités par seconde
<HitsAssembledHitsProcessedPerSecCurrent>	Current assembled hits processed per second	Nombre de hits Current traités par seconde
<HitsAssembledHitsProcessedPerSecMax>	Maximum assembled hits processed per second	Nombre maximum de hits traités par seconde
<HitsAssembledHitQueueBlocksUsedAvg>	Average assembled-hit queue blocks used	Nombre moyen de blocs de file d'attente des hits assemblés utilisés
<HitsAssembledHitQueueBlocksUsedCurrent>	Current assembled-hit queue blocks used	Blocs de file d'attente des hits assemblés Current utilisés
<HitsAssembledHitQueueBlocksUsedMax>	Maximum assembled-hit queue blocks used	Nombre maximum de blocs de file d'attente des hits assemblés utilisés

Tableau 11. Section Hits (suite)

XML	Ecran de console	Description
<HitsAssembledHitQueueCurrentBlocksUsedPct>	>Current assembled-hit queue blocks used percent	Pourcentage de blocs de file d'attente des hits assemblés Current utilisés
<HitsAssembledHitQueueCurrentEntriesUsedPct>	Current assembled-hit queue entries used percen	Pourcentage des éléments de file d'attente des hits assemblés Current utilisés
<HitsAssembledHitQueueEntriesUsedAvg>	Average assembled-hit queue entries used	Nombre moyen d'éléments de file d'attente des hits assemblés utilisés
<HitsAssembledHitQueueEntriesUsedCurrent>	Current assembled-hit queue entries used	Eléments de file d'attente des hits assemblés Current utilisés
<HitsAssembledHitQueueEntriesUsedMax>	Maximum assembled-hit queue entries used	Nombre maximum d'éléments de file d'attente des hits assemblés utilisés
<HitsAssembledHitQueueTotalAllocation Failures>	Total assembled-hit queue allocation failures	Nombre d'échecs d'allocation de file d'attente des hits assemblés • Cette statistique s'affiche comme la valeur `If non-zero, hits are being lost due to pipelined being overloaded` dans l'onglet Récapitulatif. Voir «Console Web de la PCA - Onglet Récapitulatif», à la page 60.
<HitsAssembledHitQueueTotalMisses>	Total assembled-hit queue misses	Nombre de hits assemblés manquants dans la file d'attente
<HitsAssembledHitQueueTotalPushFailures>	Total assembled-hit queue push failures	Nombre d'échecs d'envoi de hits assemblés de la file d'attente
<HitsAssembledHitQueue2TotalAllocationFailures>	Total assembled-hit queue2 allocation failures	Nombre total de hits n'ayant pas été en mesure d'allouer de l'espace dans la file d'attente entre le(s) pipeline(s) et le processus tcld. Les valeurs normales sont de zéro ou un nombre qui n'augmente pas. Vous pouvez utiliser des valeurs pour indiquer lorsque le processus tcld est surchargé. • Disponible dans PCA Build 3403 ou supérieure. • Cette statistique s'affiche comme la valeur `If non-zero, hits are being lost due to pipelined being overloaded` dans l'onglet Récapitulatif. Voir «Console Web de la PCA - Onglet Récapitulatif», à la page 60.

Tableau 11. Section Hits (suite)

XML	Ecran de console	Description
<HitsAssembledHitQueue2TotalPushFailures>	Total assembled-hit queue 2 push failures	Nombre total de hits n'étant pas parvenus à s'insérer dans la file d'attente entre le(s) pipeline(s) et le processus tcld. Les valeurs normales sont de zéro ou un nombre qui n'augmente pas. Vous pouvez utiliser cette valeur pour indiquer si le processus tcld est surchargé. **Remarque :** cet élément est disponible dans PCA Build 3403 ou supérieure.
<AveragePageSize>	Average page size	Taille moyenne de la page (type de capture 1) en octets.
<TotalPageSize>	Total page size	Utilisée pour calculer les vues de page par seconde
<PageViewsPerSecMax>	Max page views per second	Nombre maximum de vues de page par seconde.
<PageViewsPerSecCur>	Current page views per second	Vues de page Current par seconde.
<PageViewsPerSecAvg>	Average page views per second	Nombre de vues de page moyen par seconde.
<PageViewPct>	Page view percentage of hits	Pourcentage de hits correspondant à des vues de page
<HitsTotalTlapiReqNullErrors>	Total TLAPI request null errors	Nombre total d'erreurs nulles de demande TLAPI
<HitsTotalTlapiRespCorruptErrors>	Total TLAPI response corrupt errors	Nombre total d'erreurs de corruption de réponse TLAPI
<HitsTotalTlapiRespNullErrors>	Total TLAPI response null errors	Nombre total d'erreurs nulles de réponse TLAPI

Section Capture

Tableau 12. Section Capture

XML	Ecran de console	Description
<CaptureBytesWrittenByListener>	Bytes written by listener	Nombre total de paquets d'octets enregistrés par listend dans le canal de communication de reassd.
<CaptureBytesWrittenByListenerPerSec>	Bytes written by listener per second	Débit de paquets d'octets enregistrés par seconde par listend dans le canal de communication de reassd.
<CaptureBytesReadFromListener>	Bytes read from listener	Nombre total de paquets d'octets lus par reassd à partir de son canal de communication. Ce nombre doit correspondre à celui évoqué ci-dessus, enregistré par la valeur du programme d'écoute. Cette correspondance indique que listend et reassd sont synchronisés et suivent toujours le débit du trafic entrant.
<CaptureBytesReadFromListenerPerSec>	Bytes read from listener per second	Débit des paquets d'octets lu par seconde par reassd à partir de son canal de communication.
<CaptureFilteredKbytesFromPrimaryInterface>	Current filtered KB from primary interface	Nombre total de kilooctets filtrés à partir de l'interface principale.
<CaptureFilteredKbytesFromPrimaryInterfacePerSec>	Current filtered KB/sec from primary interface	Nombre de kilooctets Current filtrés par seconde à partir de l'interface principale.
<CaptureFilteredKbytesFromPrimaryInterfacePerSecMax>	Maximum filtered KB/sec from primary interface	Nombre maximal de kilooctets par seconde filtrés à partir de l'interface principale.

Tableau 12. Section Capture (suite)

XML	Ecran de console	Description
<CaptureFilteredKbytesFromSecondaryInterface>	Current filtered KB from secondary interface	Nombre total de kilooctets filtrés à partir de l'interface secondaire.
<CaptureFilteredKbytesFromSecondaryInterfacePerSec>	Current filtered KB/sec from secondary interface	Nombre de kilooctets Current filtrés à partir de l'interface secondaire.
<CaptureFilteredKbytesFromSecondaryInterfacePerSecMax>	Maximum filtered KB/sec from secondary interface	Nombre maximal de kilooctets par seconde filtrés à partir de l'interface secondaire.
<CaptureTotalPacketsRcvd>	Total packets rcvd	Nombre total de paquets reçus par pcap comme l'indiquent ses statistiques.
<CapturePacketsDroppedByPcap>	Total packets dropped by pcap	Nombre total de paquets abandonnés par pcap comme l'indiquent ses statistiques. Cette valeur doit être de zéro. Cela indique que le système d'exploitation suit toujours l'interface de carte interface réseau recevant le trafic réseau.
<CapturePacketsDroppedInOutput>	Packets dropped in output	Nombre total de paquets abandonnés par listend lorsque sa mémoire tampon de sortie est pleine. Cette valeur doit être de zéro. Cela indique que listend suit toujours le trafic réseau filtré et que reassd est en mesure d'extraire les paquets de la mémoire tampon de sortie de listend sans la surcharger.
<CaptureTotalPacketsCaptured>	Total packets captured	Nombre total de paquets capturés sur les paquets filtrés envoyés à listend par pcap.
<CaptureTotalPacketsCapturedPerSec>	Total packets captured per second	Débit des paquets filtrés reçus par seconde par pcap en provenance de listend.
<CaptureTotalIpChecksumErrors>	Total IP checksum errors	Nombre d'erreurs de total de contrôle de l'en-tête IP.
<CaptureTotalLargePacketsExceeded>	Total large packets exceeded	Nombre total de paquets TCP dont la taille dépasse la limite spécifiée. • Vous pouvez configurer la limite de la taille des paquets TCP dans la section Paramètres d'optimisation de l'onglet Interface. Voir «Console Web de la PCA - Onglet Interface» , à la page 71.
<CaptureCurrentFilteredKbytesPerSec>	Current filtered kbytes per second	Affiche le débit du trafic de kilooctets actuel par seconde en fonction du trafic de capture filtré à partir des ports de la plage. Cette statistique vous fournit des informations sur le trafic après la mise en place du filtrage et sur le volume du trafic traité par les processus de capture. Si la configuration de la carte d'interface réseau du port de la plage est définie à 100 Mbits par seconde, le débit maximal du trafic pouvant être filtré est d'environ 10 000 Ko par seconde. Ces statistiques sont mises à jour toutes les 5 secondes.
<CaptureMaxFilteredKbytesPerSec>	Maximum filtered kbytes per second	Affiche le débit maximal du trafic de kilooctets par seconde en fonction du trafic de capture filtré à partir des ports de la plage. Cette statistique vous fournit des informations sur le trafic après la mise en place du filtrage et sur le volume du trafic traité par les processus de capture. Si la configuration de la carte d'interface réseau du port de la plage est définie à 100 Mbits par seconde, le débit maximal du trafic pouvant être filtré est d'environ 10 000 Ko par seconde. Ces statistiques sont mises à jour toutes les 5 secondes.
<DeliveryMode>	Delivery Mode	Mode de distribution Current
<CoreDumps Count="0" /?>	indisponible	Nombre d'images-mémoire

Section Destinataires cible

Tableau 13. Section Destinataires cible

XML	Ecran de console	Description
<TotalHitsQueued>	Total hits queued	Nombre total de hits en attente de distribution pour le serveur IBM Tealeaf CX.

Tableau 13. Section Destinataires cible (suite)

XML	Ecran de console	Description
`<TotalHitsDelivered>`	`Total hits delivered`	Nombre total de hits distribués au serveur IBM Tealeaf CX. Ce nombre doit correspondre aux hits en attente, indiquant que la distribution des hits se poursuit.
`<TotalBytesDelivered>`	`Total bytes delivered`	Nombre total d'octets envoyés successivement au service de transport Tealeaf destinataire.
`<TotalHitsDropped>`	`Total hits dropped`	Nombre total de hits supprimés en raison d'une surcharge de la file d'attente de livraison de chaque destinataire. Cela se produit lorsque Passive Capture n'est pas en mesure de distribuer les hits au service de transport Tealeaf destinataire. Il est possible que ces échecs soient liés à des erreurs réseau (par exemple configuration du réseau de Passive Capture ou de la machine destinataire), ou à toute autre condition liée au logiciel, par exemple lorsque le service de transport Tealeaf ne fonctionne pas pendant une période prolongée. Les hits comptés par cette valeur n'ont pas été envoyés au service de transport Tealeaf.
`<UseSslText>`	`Use SSL`	Etat de la connexion de distribution SSL ou autre. • `Yes` : la connexion de distribution utilise une connexion SSL • `No` : la connexion de distribution n'est pas une connexion SSL

Section Reprise

Tableau 14. Section Reprise

XML	Ecran de console	Description
`<FailoverNodeRole>`	`Node role`	Maître ou esclave
`<FailoverNodeState>`	`Node state`	Etat actuel du noeud • `Active` : il possède le contrôle, capture des hits et les envoie en aval. • `Ready` : il capture mais n'envoie pas les hits. Il est prêt à prendre le contrôle si nécessaire. • `Down` : il ne peut pas prendre le contrôle.

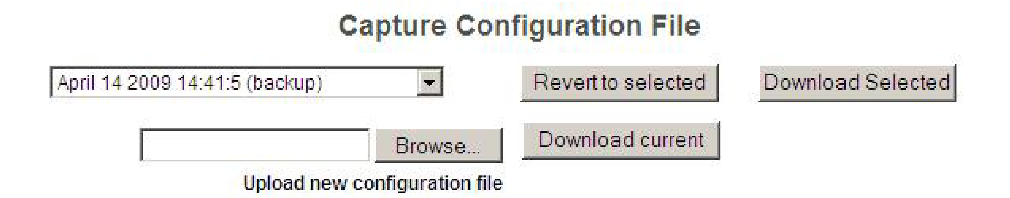
Tableau 14. Section Reprise (suite)

XML	Ecran de console	Description
<FailoverCaptureState>	Capture state	Indique si les services de capture sont en cours d'exécution sur le noeud. • Running : indique que les services de capture sont en cours d'exécution. • Stopped : les services de capture ne sont pas en cours d'exécution lorsque l'état est "stopped". • Restarting : indique que les services de capture sont en cours de redémarrage.
<FailoverActive>	Failover active	Indique si une reprise a eu lieu et si le noeud esclave actuel possède le contrôle.

Console Web de la PCA - Onglet Journaux de sauvegarde

A l'aide de l'onglet **Sauvegarde/Journaux**, vous pouvez apporter des modifications de configuration, gérer les journaux et activer l'archivage des données de paquet brutes capturées par la PC. Lors de l'enregistrement des modifications apportées à un fichier de configuration, une copie de l'ancien fichier est enregistrée dans un fichier de sauvegarde. Un message d'erreur s'affiche si la copie n'a pas abouti.

Fichier de configuration Capture



Le fichier de configuration Capture permet de modifier le fichier de configuration (`ctc-conf.xml`) via une interface Web au lieu d'utiliser un éditeur de texte. Les utilisateurs peuvent restaurer, télécharger le fichier de configuration en cours ou un nouveau fichier de configuration en cliquant sur les boutons correspondants dans la section Fichier de configuration Capture de la page.

Fichier de configuration de confidentialité

Privacy Configuration File

February 19 2009 14:28:48 (backup) | Revert to selected | Download Selected

Browse... | Download current

Upload new privacy configuration file

Cette section permet l'édition directe du fichier `privacy.cfg`, qui sert à définir les règles, tests et actions rendant les données sensibles privées avant qu'elles soient traitées par Tealeaf. Vous pouvez passer en revue les versions précédentes du fichier et télécharger de nouvelles versions à des fins d'utilisation par la PCA.

Cette version du fichier `privacy.cfg` est une copie de la version utilisée par l'agent de session pipeline Windows. Pour plus d'informations sur son contenu et son format, voir "Agent de session de confidentialité" dans le *manuel de configuration d'IBM Tealeaf CX*.

Pour plus d'informations sur la façon dont Tealeaf gère la confidentialité, voir "Gestion de la confidentialité des données" dans le *manuel de configuration d'IBM Tealeaf CX*.

Journaux

Logs (/usr/local/ctccap/logs)

View last 200 lines of log.

Capture Log | Access Log | SSL Request Log

Error Log | Configuration Changelog | Maintenance Log

You may also manage capture logfiles, configuration files, and console logfiles.

Vous pouvez accéder aux journaux PCA suivants via l'onglet **Sauvegarde/ Journaux** :

- Journal de capture
- Historique des accès
- Journal des demandes SSL
- Journal des erreurs
- Journal des modifications de configuration
- Journaux de maintenance

Dans la partie inférieure de la section Journaux, vous pouvez également accéder aux types de fichiers suivants et les télécharger :

- Fichiers journaux de Capture
- Fichiers de configuration
- Fichiers journaux de la console

Enregistrement d'archive

Dans la section relative à l'enregistrement d'archive, vous pouvez activer l'enregistrement d'archive, qui distribue des paquets capturés bruts qui ont été acheminés vers le serveur PCA dans le répertoire spécifié.

Remarque : Cette fonction est destinée au débogage. Activez-la uniquement si vous détectez des problèmes au niveau de la fonctionnalité de capture de base.

Tableau 15. Paramètres d'archivage

Paramètre	Description
`Directory`	Si cette zone est à blanc, elle est paramétrée par défaut sur `/usr/local/ctccap/archive`. Les balises `<RecordingDirectory>` et `</RecordingDirectory>` sont supprimées de `ctc-conf.xml`.
`Max archive size`	Indique la taille cumulative maximale des fichiers archive `tcpdump`. La valeur par défaut est 500 Mo. Lorsque l'utilisation de disque atteint cette valeur, les anciens fichiers archive sont supprimés afin de laisser de la place pour les nouveaux.

Pour activer l'enregistrement d'archive, cliquez sur **Archive**.

Console Web de la PCA - Onglet Reprise

A partir de l'onglet **Reprise**, vous pouvez activer et configurer la reprise entre plusieurs serveurs IBM Tealeaf Application de capture passive CX.

- Lorsqu'elle est activée, la reprise de la PCA est contrôlée par le processus de reprise dans IBM Tealeaf Application de capture passive CX.
- Pour plus d'informations sur le traitement des incidents, voir section "Traitement des incidents - Capture" du *Guide de dépannage d'IBM Tealeaf*.

Pulsations

Heartbeat:
Heartbeat Interval: 10 secs
Heartbeat Timeout: 5 secs
Timeout Limit: 3 secs

Auto Settings:
Auto Failback
Failover on SVC Restart
Failback Delay: 20

Figure 36. Pulsations pour la reprise

La machine subordonnée vérifie l'intégrité de la machine maître en lui envoyant des signaux de présence. Techniquement, ces diagnostics d'intégrité sont des demandes effectuées auprès de la machine maître pour vérifier son état actuel.

Ce signal est une demande envoyée par le biais d'un protocole de datagramme utilisateur (UDP). Lorsque la machine maître voit le signal, elle répond à l'émetteur en indiquant son état actuel. Elle envoie également des signaux de présence à la machine hôte Passive Capture subordonnée pour effectuer le suivi de son état afin de déterminer si elle peut basculer vers cette dernière.

Paramètre
: **Description**

Intervalle de signal de présence
: Indique le temps d'attente entre les pulsations.

Dépassement du délai d'attente de signal de présence
: Indique le délai d'attente de Passive Capture avant que la réponse à une pulsation n'expire.

Limite de dépassement du délai d'attente
: Indique le nombre de dépassements du délai d'attente consécutifs autorisés avant un basculement forcé.

Paramètres automatiques

Paramètre
: **Description**

`Auto Failback`
: Cette option transfère le contrôle (état actif) de la machine hôte esclave de Passive Capture à la machine hôte maître une fois que cette dernière est prête à reprendre le contrôle.

`Failover on SVC Restart`
: Cette option détermine si une reprise est déclenchée lorsque les services de capture redémarrent sur le serveur de la PCA actif.

`Failback Delay`
: Représente le délai minimum (en secondes) avant d'effectuer une reprise par restauration automatique.

Contrôleurs à distance

Dans la configuration Contrôleurs à distance, vous pouvez définir une liste de serveurs autorisés à accéder à la PCA pour contrôler les informations sur l'état de la reprise, contrôler le mode de reprise ou les deux.



Figure 37. Contrôleurs à distance

Un contrôleur à distance est un ordinateur Linux identifié par un nom d'hôte ou une adresse IP et autorisé à recevoir les informations concernant l'état de la reprise, et/ou à contrôler une machine hôte de Passive Capture configurée pour la reprise.

Remarque : ce poste de travail à distance ne doit pas être un serveur de la PCA.

Un contrôleur peut éventuellement contrôler la reprise à partir d'une machine hôte Passive Capture, notamment forcer la reprise et la reprise par restauration. Une version d'IBM Tealeaf Application de capture passive CX configurée pour la reprise répond à des pulsations ou à des demandes de contrôle envoyées par une machine correctement configurée comme un contrôleur à distance.

- Une fois que l'hôte a reçu l'autorisation, l'utilitaire des statistiques d'échec installé sur l'hôte peut être utilisé pour le débogage des problèmes liés à la reprise.

Console Web de la PCA - Onglet Utilitaires

L'onglet **Utilitaires** permet d'accéder aux informations de diagnostic du système d'exploitation, ce qui est utile si vous n'avez pas accès à PUTTY. Lorsque vous cliquez sur un bouton de commande, la sortie est générée et affichée à l'écran.

- Lorsque le mode prolixe est activé, la sortie générée peut contenir des informations supplémentaires.

Interfaces réseau

La section Interfaces réseau de l'onglet Utilitaires affiche les interfaces, les indicateurs, l'état et les adresses IP du réseau.

Network Interfaces

Interface	Flags	Status	IP Addresses
sit0 (details)	up	none	::127.0.0.1/96
eth0 (details)	up	none	fe80::20c:29ff:fe32:7981/64
eth1 (details)	up	none	fe80::20c:29ff:fe32:798b/64
lo (details)	up	none	::1/128
sit0 (details)	up	none	none
eth0 (details)	up	none	10.10.39.172/0xFFFF0000
eth1 (details)	up	none	192.168.96.128/0xFFFFFF00
lo (details)	up	none	127.0.0.1/0xFF000000

Figure 38. Console Web - Onglet Utilitaires - Interfaces réseau

Cette section répertorie toutes les interfaces réseau importantes qui comprennent les interfaces principale et secondaire ainsi que l'interface LAN utilisée pour la connexion au service de transport Tealeaf sur le serveur IBM Tealeaf CX.

- Dans les builds antérieures, cette section était affichée dans l'onglet **Récapitulatif** ou **Distribution**.

Cette section contient également les informations concernant les cartes d'interface réseau, comme les supports pris en charge et les statistiques sur les paquets.

- Pour afficher ces statistiques, cliquez sur **(détails)** à côté du nom de l'interface. Voir «Page Détails».

Paramètre
: **Description**

`Interface`
: Indique l'identificateur d'interface.

`Indicateurs`
: Les problèmes spécifiques sont répertoriés ici.
  - `up` indique que l'interface fonctionne correctement.

`Statut`
: Indique l'état tel qu'il est signalé par l'interface.

`Adresse IP`
: Indique l'adresse IP de l'interface.

Page Détails

A partir de la page Détails, vous pouvez exécuter une ligne de commande Linux ainsi que des commandes Tealeaf dans des interfaces individuelles afin d'extraire les données de diagnostic.

Remarque : le temps d'exécution de ces commandes varie en fonction de l'interface et de votre charge de trafic.

Note: Please allow time for commands to complete, e.g., bwMon, tcpdump.

bwMon | Ethtool | Ifconfig | Tcpdump | Enable verbose output.

Ifconfig Statistics and Output

```
Iface   MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0      1500   0 155769476      0      0      0        0      0      0      0 BMRU

eth0      Link encap:Ethernet  HWaddr 00:60:B0:1B:3B:36
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:155769476 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2549680435 (2431.5 Mb)  TX bytes:0 (0.0 b)
```

Figure 39. Onglet Utilitaires - Page Détails

L'image ci-dessus représente le résultat d'une commande `Ifconfig`. Pour exécuter l'une des commandes Linux disponibles, cliquez sur le bouton correspondant.

- Pour générer une sortie plus prolixe, cochez la case.

Les boutons suivant exécutent les commandes Linux pour l'interface sélectionnée :

- Ethtool
- Ifconfig
- Tcpdump

Pour plus d'informations sur les commandes, entrez `man` sur la ligne de commande Linux pour afficher la documentation disponible.

- Vous pouvez également consulter l'aide en ligne de Tealeaf pour d'autres utilisations de ces commandes concernant IBM Tealeaf Application de capture passive CX.

bwMon

Fourni par Tealeaf, l'outil bwMon génère un ensemble de statistiques de contrôle pour l'interface sélectionnée. Cette commande interroge l'interface pendant 10 secondes et renvoie les résultats à une seconde d'intervalle à partir de l'interface.

Vous pouvez utiliser cet outil avec des activités lancées dans l'application Web contrôlée pour le diagnostic des problèmes de connexion et de transfert. Par exemple, vous pouvez effectuer des actions dans l'application Web et vérifier si elles ont déclenché des activités par le biais de l'interface appropriée.

- La case à cocher Activer sortie prolixe génère le même ensemble de statistiques.

Un exemple de sortie s'affiche, dans lequel une ligne correspond à un intervalle d'une seconde pour une requête de 10 secondes.

- Si aucun trafic n'est transmis à l'instance, la sortie contient uniquement la liste des noms de zone.

Note: Please allow time for commands to complete, e.g., bwMon, tcpdump.

bwMon | Ethtool | Ifconfig | Tcpdump | Enable verbose output.

bwMon Output

```
Time,Dev,Mbs,rxbytes,rxpkts,rxerrs,rxdrop
23:09:54:19,eth3,0,2653532987,661989560,0,0
23:09:54:20,eth3,0,2653537369,661989576,0,0
23:09:54:21,eth3,0,2653539661,661989587,0,0
23:09:54:22,eth3,0,2653540602,661989596,0,0
23:09:54:23,eth3,0,2653541107,661989600,0,0
23:09:54:24,eth3,0,2653541943,661989607,0,0
23:09:54:25,eth3,0,2653542934,661989614,0,0
23:09:54:26,eth3,0,2653543725,661989622,0,0
23:09:54:27,eth3,0,2653544432,661989628,0,0
23:09:54:28,eth3,0,2653545417,661989640,0,0
```

Figure 40. Exemple de sortie bwMon

Zone	Description
Heure	Indique l'horodatage de l'intervalle d'une seconde sélectionné
Dev	Correspond à l'unité interrogée
Mo/s	Indique la vitesse de transfert en mégabits par seconde entre l'unité et IBM Tealeaf Application de capture passive CX. • Une valeur de 0 peut signaler une unité inactive ou un problème de configuration.
rxbytes	Indique le volume d'octets transférés de l'unité vers la PCA.
rxpkts	Indique le volume de paquets transférés de l'unité vers la PCA.
rxerrs	Indique le nombre d'erreurs de transfert de l'unité vers la PCA.
rxdrop	Indique le nombre de paquets abandonnés par l'unité.

Utilitaires du système

Les utilitaires du système, que vous trouverez au bas de l'onglet **Utilitaires**, permettent de générer des informations importantes de diagnostic concernant la PCA, le système d'exploitation qui l'héberge et les statistiques générées par la PCA.

System Utilities

Note: Please allow time for commands to complete, e.g., Statistics Summary, Top.

Miscellaneous Bootlog Config Diffs Dmesg Ifconfig Tealeafenv

Processes All Capture Top

Statistics Raw Format Summary XML Format

Enable verbose output.

Figure 41. Console Web - Onglet Utilitaires - Utilitaires du système

Utilitaire
: **Description**

Divers

Bootlog
: Permet de consulter le fichier journal bootlog Linux du système qui héberge la PCA.

Config Diffs
: Permet de voir les différences entre le fichier de configuration par défaut (`ctc-conf-defaults.xml`) et la configuration actuelle (`ctc-conf.xml`).

Dmesg
: Permet d'exécuter la commande Linux `dmesg` qui affiche les informations concernant la mémoire tampon tournante du noyau.

Ifconfig
: Permet d'exécuter la commande `Ifconfig` sur chacune des interfaces réseau.

Tealeafenv
: La commande Tealeafenv génère des informations spécifiques à l'installation de la PCA de Tealeaf.

Processus
: Ces commandes génèrent des informations statistiques sur les processus Linux en cours d'utilisation.

Tout
: Permet de consulter tous les processus système pour tous les utilisateurs.

Capture
: Permet de consulter tous les processus en cours d'utilisation par l'utilisateur d' IBM Tealeaf Application de capture passive CX (généralement `ctccap`).

Haut
: Permet d'exécuter le programme `top` pour Linux. `top` affiche en temps réel les informations récapitulatives du système ainsi qu'une liste des tâches en cours gérées par le noyau Linux.

Statistiques
: Ces commandes génèrent des statistiques relatives à IBM Tealeaf Application de capture passive CX.

Format brut
: Permet de consulter les statistiques au format brut.

Récapitulatif
: Permet de consulter les statistiques de chaque instance de la PCA.

Format XML
: Permet d'afficher les statistiques de la PCA en XML. Pour plus d'informations sur ces statistiques, voir «Statistiques par instance», à la page 137.

Console Web de la PCA - Page Débogage

Vous pouvez gérer les fichiers d'image-mémoire principaux à partir de la page Débogage de la console Web de la PCA. Vous pouvez télécharger, supprimer ou déboguer les images-mémoire produites lors des opérations de la PCA.

- A partir de la page Débogage, vous pouvez également télécharger des fichiers compressés à transmettre au service clients Tealeaf. Voir «Fichier ZIP de la PCA pour bénéficier du support», à la page 170.

Accès à la page Débogage

Remarque : Pour des raisons de sécurité, vous devez vous connecter à la console Web par le biais d'une connexion SSL et activer l'authentification d'utilisateur doit être activée afin de télécharger les fichiers.

Lorsque les images-mémoire sont créées, un message accompagné d'un lien s'affiche dans l'onglet **Récapitulatif**. Pour ouvrir la page Débogage, cliquez sur le lien **Afficher**.

- Voir «Console Web de la PCA - Onglet Récapitulatif», à la page 60.

Accès direct à la page Débogage de la console Web de la PCA :

```
https://<host_name>:8443/debug.php
```

où :

- <host_name> est l'hôte de la PCA.

Page Présentation

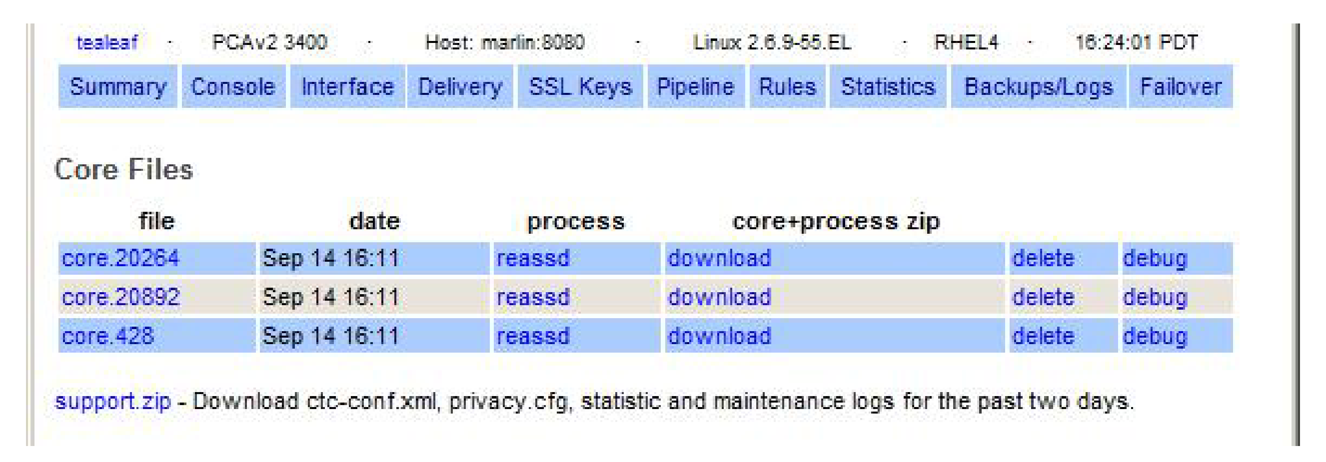


Figure 42. Console Web de la PCA - page de débogage

Remarque : Si vous n'êtes pas connecté via SSL et n'utilisez pas l'authentification, certaines des actions suivantes sont désactivées.

Zone **Description**

fichier
: Indique le nom du fichier d'image-mémoire principal.

date
: Indique la date de création de l'image-mémoire (et de la panne)

processus
: Indique le processus en panne qui a créé l'image-mémoire.

zip noyau+processus
: Fournit un lien pour télécharger l'image-mémoire et le processus dans un fichier compressé unique.

supprimer
: Cliquez sur ce lien pour supprimer le fichier core.

  Remarque : cette commande est utile lorsque la partition sur l'unité de disque dur contenant la PCA est pleine.

débogage
: Permet d'exécuter un débogage simple du vidage. Voir «Sortie de débogage».

Sortie de débogage

Vous trouverez ci-après un exemple de sortie de la commande de débogage :

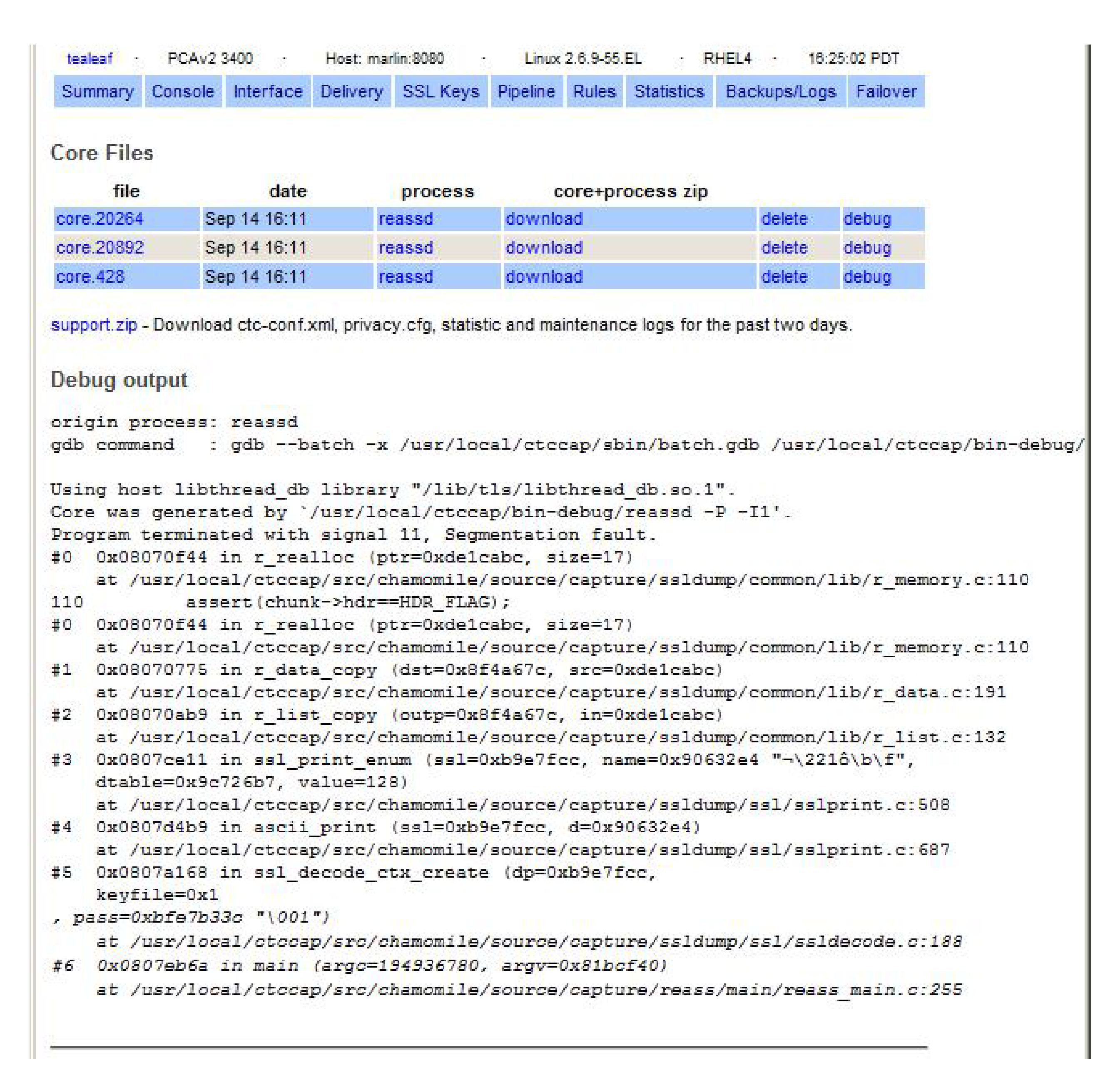


Figure 43. Sortie de la commande de débogage

Fichier ZIP de la PCA pour bénéficier du support

Lorsque vous travaillez avec le service clients et le service technique Tealeaf pour résoudre les problèmes du site d'un client, envoyez le fichier `support.zip` sur le site `debug.php` afin d'aider à résoudre le problème.

Remarque : lorsque vous fournissez des images-mémoire, précisez le type et la version de Linux sur laquelle est installée la PCA.

Contenu du fichier ZIP

1. fichier d'image-mémoire principal ;
2. fichier binaire à l'origine du vidage ;

3. `ctc-conf.xml`
4. `privacy.cfg`
5. Journaux de maintenance et de statistiques actuels et des jours précédents.

Fichier de configuration Passive Capture `ctc-conf.xml`

Si vous ne pouvez pas vous connecter à la console Web, vous pouvez éditer le fichier `ctc-conf.xml` pour configurer IBM Tealeaf Application de capture passive CX

Remarque : évitez d'effectuer des modifications directement dans ce fichier de configuration. Nous vous conseillons d'utiliser la console Web de la PCA, car elle fournit une interface utilisateur pour ce fichier de configuration. Pour plus d'informations, voir «Navigateurs pris en charge pour la console Web de la PCA», à la page 54.

Ce fichier se trouve dans le répertoire `/usr/local/ctccap/etc`. Vous pouvez le modifier à l'aide de l'éditeur **`vi`**.

Remarque : certains des paramètres ne figurent pas dans le fichier de configuration par défaut. Ces paramètres peuvent être insérés en fonction des modifications de la configuration effectuées par le biais de la console Web. Tous les paramètres de configuration nécessaires pour une utilisation générale de la PCA sont disponibles dans le fichier par défaut.

Remarque : SSH est exécuté sur le port standard 22.

Remarque : effectuez toujours une copie de sauvegarde du fichier de configuration avant toute modification.

Remarque : ne modifiez pas ce fichier de configuration ou tout autre fichier de configuration de la PCA par le biais d'un éditeur sur une machine Windows. Les caractères de fin de ligne (EOL) de Windows sont différents des fins de ligne UNIX utilisées par Linux. Par conséquent, des erreurs de configuration peuvent survenir lorsque le fichier est de nouveau appliqué à l'environnement Linux de la PCA.

Les tableaux ci-dessous expliquent chaque option de configuration du fichier de configuration par défaut.

<Conf>

Tableau 16. Paramètres de configuration

Option de configuration	Description
`<IPv6ConsoleEnabled>`	A partir de PCA Build 3600, la console Web peut être configurée afin d'accepter les adresses IPv6 par défaut. Pour activer cette option, paramétrez cette valeur sur 1. **Remarque :** Pour les systèmes qui ont été mis à niveau, vous devez insérer manuellement ce paramètre et sa valeur dans le fichier de configuration. Cette modification de configuration peut également s'appliquer à la Build 3502 de la PCA.

Tableau 16. Paramètres de configuration (suite)

Option de configuration	Description
<Timeout>	A partir de la Build 3600 de la PCA, vous pouvez affecter à ce paramètre une valeur différente de zéro afin d'activer les délais d'expiration des sessions de console Web de la PCA. La valeur indiquée définit le délai d'inactivité, en minutes, autorisé pour une session de console Web avant l'expiration automatique de la session. En fonction de votre build, ce paramètre peut ou non être présent dans cet emplacement. Faites une recherche dans le fichier. Si le paramètre n'est pas présent dans votre fichier, insérez-le ici. Pour plus d'informations, voir «Console Web de la PCA - Onglet Console», à la page 70.

<Archive>

Cette section définit les options de configuration permettant d'activer et de gérer l'archivage de paquet TCP/IP local. Pour plus d'informations, voir «Console Web de la PCA - Onglet Journaux de sauvegarde», à la page 159.

Tableau 17. Paramètres d'archivage

Option de configuration	Description
<RecordingEnabled>	Active l'archivage de paquet TCP/IP local. Lorsque ce paramètre est activé, les fichiers archive sont enregistrés dans le répertoire d'enregistrement d'archive (par défaut, `/usr/local/ctccap/archive`) dans une archive évolutive. Les archives sont partitionnées en fichiers de 50 Mo. Ce paramètre est désactivé par défaut.
<MaxSize>	Indique la taille maximale des archives de paquets TCP/IP. Par défaut, `MaxSize` a pour valeur 500 Mo. La taille de répertoire par défaut allouée aux archives est de 18 Go.
</Archive>	

<Capture>

Utilisez les paramètres de configuration de la capture pour configurer la capture des données à partir d'un port de commutation mis en miroir ou d'un TAP réseau.

Tableau 18. Paramètres de capture

Option de configuration	Description
<HangingResponseTimeout>	Indique le délai d'attente (en secondes) entre le dernier paquet de la demande et le premier paquet de la réponse. Si le délai est dépassé, la connexion est marquée comme étant annulée par le client. La valeur par défaut est de 120 secondes.

Tableau 18. Paramètres de capture (suite)

Option de configuration	Description
<HangingTransmissionTimeout>	<Indique le délai d'attente (en secondes) de Passive Capture entre les paquets. Si le délai est dépassé, la connexion est marquée comme étant une demande annulée par le client. La valeur par défaut est de 120 secondes.
<Ignores/>	
<ListenFullDuplex>	Définit si Passive Capture reçoit des données bidirectionnelles d'un TAP réseau ou des données unidirectionnelles d'un port SPAN sur un commutateur réseau ou un équilibreur de charge. Si la machine hôte Passive Capture reçoit des données d'un TAP réseau, paramétrez `ListenFullDuplex=False`. Si la machine hôte reçoit des données d'un port miroir, paramétrez `ListenFullDuplex=True`.
<ListenOnBothInterfaces>	Indique si Passive Capture est en mode écoute sur l'une de ses interfaces Ethernet ou sur les deux. Il peut servir à capturer deux ports SPAN. Si Passive Capture reçoit des données d'un TAP réseau, paramétrez `ListenOnBothInterfaces=True`. S'il reçoit des données d'un port miroir, paramétrez `ListenOnBothInterfaces=False`.
<ListenTo>	Incorporée dans la section <Capture>, cette sous-section définit l'ensemble des serveurs Web à surveiller par Passive Capture. Les attributs <Address> et <Port> doivent être configurés pour chaque serveur Web à surveiller. Passive Capture prend également en charge les masques de réseau. Si un paramètre de masque de réseau est utilisé, un noeud <NetmaskSize> doit être ajouté dans le fichier de configuration sous le noeud <Address> et avant le noeud <Port>. Par exemple, si la plage d'adresses IP des serveurs Web à surveiller est comprise entre 10.10.10.0 et 10.10.10.255 et que les serveurs Web sont mode écoute sur les ports 80 et 443, la configuration de `ListenTo` se présente comme suit : <ListenTo> <Address>10.10.10.0</Address> <NetmaskSize>24</NetmaskSize> <Port>80</Port> <Port2>443</Port2> </ListenTo> Pour plus d'informations sur les meilleures pratiques de gestion des adresses IP, voir «Navigateurs pris en charge pour la console Web de la PCA», à la page 54.
<ListenTos>	
<Address>	Indique l'adresse IP du serveur Web qui est en cours de surveillance.
<Port>	Indique le numéro de port d'écoute du serveur Web.
<Port2>	Indique un numéro de port supplémentaire associé à l'attribut Address. Optimisé pour la surveillance standard à deux ports.

Tableau 18. Paramètres de capture (suite)

Option de configuration	Description
<NetMaskSize>	Indique la plage d'adresses IP à surveiller, via la taille de masque de réseau en bits.
</ListenTo>	
</ListenTos>	
<MaxSimultaneousConnections>	Définit le nombre maximal de connexions TCP simultanées pouvant être traitées par le logiciel Passive Capture. La valeur par défaut est de 10000.
<MaxConnectionsInSynState>	Définit le nombre maximal de connexions TCP simultanées dans lesquelles des connexions TCP partielles sont établies. La valeur par défaut est 4000.
<PrimaryInterface>	Indique le nom de l'interface Ethernet principale. La valeur par défaut est `eth0`.
<SecondaryInterface>	Indique le nom de l'interface Ethernet secondaire.
<MaxSessionCacheSize>	Définit le nombre maximal de connexions SSL simultanées pouvant être traitées. La valeur par défaut est de 10 000.
<MaxInputBufferSize>	**Remarque :** Ne modifiez pas ce paramètre sans avoir au préalable contacté l'assistance technique. Ce paramètre est utilisé pour déboguer les problèmes liés aux pics de trafic entraînant une surcharge de la mémoire tampon.Définit la taille maximale (en octets) de la file d'attente de traitement des paquets TCP. La valeur par défaut est de 100 000 000 (environ 100 Mo). Quand la mémoire tampon se remplit, la PCA commence à abandonner les hits. La limite de la mémoire tampon permet d'éviter que le système ne tombe en panne. Cependant, certaines données sont supprimées.
<MaxMemoryConsumption>	**Remarque :** Ne modifiez pas ce paramètre sans avoir au préalable contacté l'assistance technique. Ce paramètre est utilisé pour déboguer les problèmes liés aux pics de trafic entraînant une surcharge de la mémoire tampon.Permet de définir la quantité maximale de mémoire système (en Mo) allouée au processus de capture. La valeur par défaut est de 1300 Mo (1,3 Go). IBM Tealeaf Passive Capture Application est une application 32 bits, ce qui signifie que chaque processus de la CX PCA peut gérer un maximum de 2 Go de mémoire RAM.

Tableau 18. Paramètres de capture (suite)

Option de configuration	Description
<TransparentLoadBalancingEnabled>	Active ou désactive la fonction d'équilibrage de charge transparent (TLB). Pour activer l'équilibrage de charge, paramétrez TransparentLoadBalancingEnabled sur True. Pour le désactiver, paramétrez TransparentLoadBalancingEnabled sur False. La valeur par défaut est True, ce qui active l'équilibrage de charge. Pour plus d'informations, voir «Présentation de l'équilibrage de charge transparent de d'CX PCA», à la page 8.
<ReassInstances>	Configure le nombre d'instances reassd à créer. La valeur par défaut est 1.
<SslSessionInfoOnMemcachedServer>	Si l'équilibrage de charge transparent est activé et que SslSessionInfoOnMemcachedServer paramétré sur True, la PCA utilise memcache pour mettre en mémoire cache les données SSL. La valeur par défaut de SslSessionInfoOnMemcachedServer est True.
<MemcachedServerIP>	Définit l'adresse IP ou le nom d'hôte à utiliser pour le service memcache. La valeur par défaut est localhost.
<MemcachedServerPort>	Définit le numéro de port du service memcache. La valeur par défaut est 11211.
<MemcachedServerMemory>	Définit l'espace mémoire, en Mo, qui est alloué pour le service memcache. La valeur par défaut est de 256 Mo.
<RestartMemcache>	Définit si le service memcache est redémarré lors du redémarrage du service PCA, ce qui vide les paquets SSL mis en cache. Pour activer cette fonction, paramétrez la valeur sur True. La valeur par défaut est False.
<MaxConnectionsRoutingInfo>	Définit la quantité d'informations de routage de connexion TCP pouvant être stockées dans la table de hachage routerd locale. Une fois la limite atteinte, les anciennes données sont supprimées de la table de sorte qu'une nouvelle valeur puisse être écrite dans la table. La valeur par défaut est 100000.
<MaxInputRouterdBufferSize>	Définit la taille de mémoire tampon, en Mo, pour le service routered. La valeur par défaut est de 50 Mo.

Tableau 18. Paramètres de capture (suite)

Option de configuration	Description
<DeleteTcpLargeConnDisabled>	Ce paramètre est un indicateur booléen, paramétré sur `True` ou sur `False`. S'il n'est pas spécifié, il est traité comme s'il était paramétré sur False. S'il a pour valeur `True`, ce paramètre empêche la fermeture des connexions TCP dont la taille des demandes ou réponses individuelles est dépassée. Dans des cas particuliers, tels que des fichiers pdf ou des connexions de trafic en flux, il est peut-être nécessaire de désactiver cette fonction pour maintenir la connexion. La taille maximale des demandes ou réponses individuelles est définie par le paramètre `MaxTcpConnSize`.
<MaxTcpConnSize>	Taille maximale autorisée d'une demande ou réponse individuelle dans une connexion TCP. Une connexion TCP unique peut comporter plusieurs demandes ou réponses, chacune étant vérifiée quant à cette limite. La valeur par défaut est 2097152. Si cette limite est dépassée, la connexion TCP est automatiquement fermée lorsque `DeleteTcpLargeConnDisabled` est paramétré sur `False`.
<CaptureKeys/>	
<CaptureKey>	Cette section facultative sert à définir les clés SSL nécessaires pour la prise en charge de la capture du trafic HTTPS à partir de serveurs Web. • Pour chaque clé privée, une section CaptureKey incluant les noeuds `<CertificateFile>` (facultatif), <Label> et `<PrivateKeyFile>` doit être définie. • Les entrées `<CertificateFile>` et `<PrivateKeyFile>` correspondent aux noms de domaine qualifiés des fichiers contenant le certificat et les clés privées. • Pour pouvoir être utilisée, la clé privée doit être au format `.PTL` converti par Tealeaf.
<Certificate>	Définit l'emplacement dans lequel la clé publique doit être collée.
<Label>	Indique le nom textuel de la clé privée.
<PrivateKey>	Définit l'emplacement dans lequel la clé privée doit être collée.
</CaptureKey>	
</CaptureKeys/>	
<InstancesEnabled>	Ce paramètre fournit un paramètre global permettant d'activer/désactiver plusieurs instances. Ce paramètre est un indicateur booléen, paramétré sur `True` ou sur `False`. • S'il n'est pas spécifié, il est traité comme s'il était paramétré sur `False`. • S'il est paramétré sur `True`, le noeud `<Instances>` imbriqué ci-dessous est utilisé pour l'instanciation de plusieurs instances. Dans le cas contraire, une seule instance est créée.

Tableau 18. Paramètres de capture (suite)

Option de configuration	Description
<Instances>	Noeud de niveau supérieur pour les définitions imbriquées comportant plusieurs instances.
<Instance>	Noeud Instance permettant la définition des attributs d'une instance.
<InstanceDisabled>	Ce paramètre est un indicateur booléen, paramétré sur True ou sur False. • S'il n'est pas spécifié, il est traité comme s'il était paramétré sur False. • S'il est paramétré sur True, le noeud Instance local est désactivé. En désactivant le noeud Instance, vous pouvez désactiver des instances individuelles à des fins de débogage ou de test.
<ListenFullDuplex>	Si ce paramètre est défini dans le noeud Instance, il a la même signification que l'instance principale précédente, mais ce paramètre s'applique à cette instance particulière. S'il n'est pas défini, l'instance hérite de la valeur de l'instance principale. Paramétrez <ListenFullDuplex> sur True ou sur False.
<ListenOnBothInterfaces>	Si ce paramètre est défini dans le noeud Instance, il a la même signification que l'instance principale précédente, mais ce paramètre s'applique à cette instance particulière. S'il n'est pas défini, l'instance hérite de la valeur de l'instance principale. Paramétrez <ListenOnBothInterfaces> sur True ou sur False.
<TcpChecksumDisabled>	Par défaut, la CX PCA exécute une validation de total de contrôle des paquets TCP qui lui sont soumis. Les environnements dans lesquels un système LRO (Large Receive Option) ou le déchargement du total de contrôle est activé, la validation de total de contrôle de la PCA échoue. Paramétrez la valeur sur True pour le désactiver. Si ce paramètre ne figure pas dans le XML par défaut, la CX PCA suppose que la validation de total de contrôle est souhaitée et activée. Ce paramètre apparaît dans le XML une fois que la validation de total de contrôle des paquets est désactivée via l'onglet Interface de la console Web de la PCA en cochant la case de validation **Désactiver le total de contrôle des paquets**. Pour plus d'informations, voir «Console Web de la PCA - Onglet Interface», à la page 71.
<PipelineInstances>	Indique le nombre de processus pipeline (pipelined) permettant de créer un système pouvant prendre en charge plusieurs pipelines. Vous pouvez ajouter un processus pipelined supplémentaire pour chaque coeur de processeur supplémentaire inactif. Par défaut, cette valeur est paramétrée sur 1. Pour plus d'informations sur la création de plusieurs pipelines, voir «Console Web de la PCA - Onglet Pipeline», à la page 101.

Tableau 18. Paramètres de capture (suite)

Option de configuration	Description
<SslHwCheckDisabled>	Lorsque ce paramètre à pour valeur true, la CX PCA désactive la recherche et l'utilisation de cartes accélératrices matérielles SSL. La valeur par défaut est `False`.
<MaxPipelineSHMQueueSize>	Définit la taille (en mégaoctets) de la file d'attente qui approvisionne des hits aux instances du pipeline. Par défaut, cette valeur est paramétrée sur 100 Mo. La valeur maximale admise est de 200 Mo.
<MaxPipelineSHMQueue2Size>	Définit la taille (en mégaoctets) de la file d'attente qui approvisionne des hits à partir des instances du pipeline vers le module moteur `Tcl`. Par défaut, cette valeur est paramétrée sur 100 Mo. La valeur maximale admise est de 200 Mo. Pour plus d'informations sur la création de plusieurs pipelines, voir «Console Web de la PCA - Onglet Pipeline», à la page 101.
</Capture>	

<Delivery>

Cette section inclut les attributs permettant de configurer le transfert de données en temps réel de la machine hôte Passive Capture vers l'environnement de serveur IBM Tealeaf CX.

Tableau 19. Paramètres de distribution

Option de configuration	Description
<DeliveryMode>	Configure le mode de distribution de la PCA à ses homologues. Pour plus d'informations, voir «Console Web de la PCA - Onglet Distribution», à la page 92. `<DeliveryMode>2</DeliveryMode>`
<BatchInterval>	Ce paramètre n'est pas utilisé.
<MaxQueueDepth>	Définit la taille maximale (en octets) de la file d'attente pour l'envoi de données au serveur IBM Tealeaf CX. La valeur par défaut est 0, qui paramètre le nombre de lignes de la file d'attente sur 50 Mo.
<MyCertificate>	Ce paramètre n'est pas utilisé.
<MyPrivateKey>	Ce paramètre n'est pas utilisé.
<StatisticsHitEnabled>	Ce paramètre est un indicateur booléen, paramétré sur `True` ou sur `False`. • S'il a pour valeur `True`, les hits de statistiques sont activés sous la forme d'une fonction. • S'il a pour valeur `False`, la fonction est désactivée. Si aucune valeur n'est définie, le paramètre est considéré comme ayant pour valeur `False`.

Tableau 19. Paramètres de distribution (suite)

Option de configuration	Description
<StatisticsHitHost>	Ce paramètre correspond au nom d'hôte ou à l'adresse IP de la machine qui exécute le service de transport Tealeaf qui reçoit les hits de statistiques.
<StatisticsHitIntervalSeconds>	Cette valeur, un nombre positif, représente le laps de temps minimum en secondes entre les tentatives d'envoi des hits de statistiques. Si vous indiquez 0 (zéro), les hits de statistiques ne seront pas envoyés.
<StatisticsHitPort>	Ce paramètre, un numéro de port positif, correspond au numéro de port TCP/IP à utiliser lors de la connexion au service de transport Tealeaf sur l'hôte.
<StatisticsHitSecure>	Ce paramètre, un indicateur booléen, indique si la connexion au service de transport Tealeaf est activé pour SSL. Il peut avoir pour valeur `True` ou `False`. S'il n'est pas spécifié, il est traité comme s'il était paramétré sur False.
<TimeSourceHost>	Désigne le nom de domaine ou l'adresse IP de l'hôte qui exécute le service de transport Tealeaf à utiliser comme horloge de référence. Si vous ne souhaitez pas vous synchroniser avec une horloge de référence, ne renseignez pas cette zone.
<TimeSourcePort>	Désigne le port sur lequel l'hôte de l'horloge de référence écoute les requêtes concernant l'heure. Si vous ne souhaitez pas vous synchroniser avec une horloge de référence, ne renseignez pas cette zone.
<Peers>	
<Peer>	Définit l'adresse IP et le port de l'environnement de serveur IBM Tealeaf CX destinataire. Une section <Peer> doit être définie pour chaque serveur IBM Tealeaf CX destinataire.
<Host>	Indique l'adresse IP ou le nom d'hôte du serveur IBM Tealeaf CX qui reçoit des données de la machine hôte Passive Capture.
<Port>	Indique le numéro de port IP sur le serveur IBM Tealeaf CX auquel les données sont envoyées. La valeur par défaut est 1966.
</Peers>	
<PollingInterval>	Ce paramètre n'est pas utilisé actuellement.

Tableau 19. Paramètres de distribution (suite)

Option de configuration	Description
<WatchdogTimer>	Indique le délai maximal (en secondes) autorisé pour établir une connexion au serveur IBM Tealeaf CX. Si le délai est dépassé, la connexion est marquée comme déconnectée. La valeur par défaut est de 30 secondes.
</Delivery>	
<ConfigurationChangeTime>	Indique l'heure UNIX (secondes depuis le 1e janvier 1970 en temps universel coordonné) depuis la dernière mise à jour du fichier de configuration par la console Web. **Remarque :** Ne modifiez pas ce paramètre. Ce paramètre est automatiquement modifié lorsqu'une mise à jour est effectuée via la console Web.

<Extension/>

Le paramètre <Extension/> n'est pas utilisé.

<Parse>

Les paramètres de configuration ci-dessous servent à définir les paramètres de mise en sessions pour Tealeaf Cookie Injector. Pour plus d'informations, voir «Console Web de la PCA - Onglet Pipeline», à la page 101.

Tableau 20. Paramètres d'analyse

Option de configuration	Description
<UserIDName>	(Facultatif) Indique la valeur d'en-tête HTTP(S) qui est définie par Tealeaf Cookie Injector comme attribut d'ID utilisateur. La valeur par défaut est `TLTUID`.
<SessionIDName>	Indique la valeur d'en-tête HTTP(S) qui est définie par Tealeaf Cookie Injector comme attribut d'ID session. La valeur par défaut est `TLTUID`.
<HitIDName>	Indique la valeur d'en-tête HTTP(S) qui est définie par Tealeaf Cookie Injector comme attribut d'ID hit. La valeur par défaut est `TLTUID`.
<TealeafCookies>	Indique si Tealeaf Cookie Injector est en cours d'utilisation. La valeur par défaut est `True`.

Tableau 20. Paramètres d'analyse (suite)

Option de configuration	Description
<CaptureMode>	Indique le mode de capture utilisé. Il peut comporter les deux valeurs suivantes : `Business` et `BusinessIT`. • Si `CaptureMode=Business`, le logiciel ne capture que les objets demande et réponse HTTP(S) pour les demandes de page 'business' (par exemple, `HTML`, `ASP`, `JSP`). Les objets non textuels associés ne sont pas capturés (par exemple, `GIF`, `JPEG`) sur cette page. • Si `CaptureMode=BusinessIT`, le logiciel capture également les objets demande et réponse HTTP(S) pour les objets de fichier associés à la page 'business' (par exemple, `GIF`, `JPEG`). • La valeur par défaut est `Business`.
<ExcludeExtensions>	Indique les extensions de fichier à exclure du DataStream capturé. Il est possible d'utiliser ce paramètre pour affiner le comportement défini selon le mode de capture.
<IncludeExtensions>	Indique les extensions de fichier capturées en intégralité. Il est possible d'inclure des fichiers binaires tels que les PDF.
<CaptureAllTypes>	Spécifie les types de contenu (types MIME) pour lesquels capturer un hit complet (y compris la réponse).
<IncludeMethods>	Indique les méthodes HTTP à inclure. Les valeurs par défaut sont `Get`, `Post` et `Put`.
<RawRequest>	Détermine si RawRequest est actif. RawRequest constitue une aide au débogage. La valeur par défaut est `False` (désactivé). S'il a pour valeur `True`, les en-têtes de demande HTTP sont ajoutés au hit. **Remarque :** Il est recommandé de paramétrer la valeur sur `False` pour empêcher l'ajout de données supplémentaires à chaque hit.
<ResponseHeaders>	Détermine si les en-têtes de réponse sont actifs. Ils constituent une aide au débogage. La valeur par défaut est `False` (désactivé). Lorsque ce paramètre est activé (`True`), les en-têtes de réponse HTTP sont ajoutés au hit. **Remarque :** Il est recommandé de paramétrer la valeur sur `False` pour empêcher l'ajout de données supplémentaires à chaque hit.

Tableau 20. Paramètres d'analyse (suite)

Option de configuration	Description
`<MaxResponseSize>`	Indique la taille maximale autorisée pour la réponse (en octets). La valeur par défaut est 1572864 (1,5 Mo).
`<MaxDataSizeBytes>`	Nombre maximal d'octets autorisés pour la communication entre Passive Capture et la représentation de hit binaire utilisée pour la communication avec le service de transport Tealeaf. La valeur par défaut est de 2 Mo (2097152).
`<MaxRequestSizeBytes>`	Nombre maximal d'octets autorisés pour les demandes HTTP. Si cette valeur est dépassée, le corps de la demande ou la totalité de la demande est supprimée. La valeur par défaut est de 2 Mo (2097152).
`<ShrinkToFit>`	Si ce paramètre a pour valeur `True`, le code de traitement des hits n'alloue pas d'espace supplémentaire lorsqu'il redimensionne les mémoires tampon. L'espace supplémentaire minimise les futures réallocations, ce qui augmente les performances. • Paramétrez cette valeur sur `True` uniquement si vous voulez exercer le code de traitement des hits de façon plus agressive et maintenir son utilisation de mémoire à un niveau minimal. • La valeur par défaut et recommandée est `False`.
`<InflateEnabled>`	Si une réponse possède un en-tête de codage de contenu dont la valeur est `deflate`, `gzip` ou `x-gzip`, son corps est alors susceptible d'être décompressé (développé à partir de son état compressé). • S'il a pour valeur `True`, une tentative de décompression de la réponse est effectuée. – Lorsque la décompression échoue, un message est consigné dans le journal notice. – Lorsque la décompression aboutit, la valeur de l'en-tête de codage de contenu est écrasée par le caractère X. Par exemple, l'en-tête de codage de contenu peut avoir pour valeur `XXXX`. • La valeur par défaut est `False`.
`<MoveXMLToREQ>`	Déplace le XML de la réponse vers une section XML dans la demande. **Remarque :** Cette fonction est désactivée. Quelle que soit la valeur définie, la PCA se comporte comme si cet attribut était paramétré sur `False`.

Tableau 20. Paramètres d'analyse (suite)

Option de configuration	Description
<UnReqCancelled>	Lorsqu'elle est activée, cette option vérifie les 100 derniers octets du corps de réponse pour capturetype=1 et est marquée comme annulée.
<CookieParsingEnabled>	Lorsque cette option est sélectionnée, une section de cookies est ajoutée à la demande.
<URLDecodingEnabled>	Cette option définit si les adresses des zones URL doivent être décodées.
<DelImagesEnabled>	Lorsque cette option est sélectionnée, elle active la fonction DelImages dans la PCA, qui supprime automatiquement les hits d'image répondant aux critères spécifiques. Pour plus d'informations, voir «Console Web de la PCA - Onglet Pipeline», à la page 101.
<TLISupportEnabled>	Cette option permet la capture du contenu statique par la PCA en vue de la stocker dans un serveur TLI déployé sur vos serveurs Tealeaf sous Windows. • Un serveur TLI permet la capture du contenu statique, tel que les images, les JavaScript et les feuilles de style, dans une archive permanente pour les exigences d'audit et de relecture à fidélité maximale. Pour plus d'informations, voir *IBM Tealeaf cxImpact Administration Manual*. • Lorsque cette option est activée, elle remplace la fonction DelImages dans la PCA. Pour plus d'informations, voir «Console Web de la PCA - Onglet Pipeline», à la page 101.
<SessioningEnabled>	Si cette option est définie, les hits sont regroupés dans des sessions basées sur <SessField/>.
<SessField>	Zone principale dans laquelle effectuer une mise en session. Elle doit être définie si la mise en session est activée. Cette valeur peut correspondre à n'importe quelle zone de la mémoire tampon de requête, paire nom-valeur [urlfield] ou REMOTE_ADDR dans la section [env]. Vous pouvez spécifier la zone de mise en session principale et d'autres zones sous la forme d'une liste de noms de zone délimités par des virgules. Les noms de zone dans des sections distinctes peuvent être précédés du nom de section, par exemple cookies:field1, urlfield:field2.

Tableau 20. Paramètres d'analyse (suite)

Option de configuration	Description
<SessSection>	Zone facultative identifiant la section de la mémoire tampon de requête dans laquelle la valeur SessField est trouvée. Utilisez cette zone uniquement si une section explicite n'est pas référencée dans la ou les valeurs SessField. Si cette valeur n'est pas spécifiée, une recherche est effectuée dans la totalité de la requête et la première occurrence est utilisée.
<SessFieldMaskOff>	Indique une sous-chaîne de la zone de demande SessField à utiliser pour la mise en session. Cette valeur peut correspondre à deux décalages à base zéro ou à un décalage de début et le mot end pour utiliser tous les éléments compris entre la position de début et la fin de la valeur. Par exemple : • PrimarySessFieldMaskOff=0 end utilise la totalité de la chaîne • PrimarySessFieldMaskOff=0 19 utilise les 20 premiers caractères • PrimarySessFieldMaskOff=14 end-4 utilise le 15ème caractère jusqu'au 4ème à partir de la fin • PrimarySessFieldMaskOff=end-9 end-2 utilise le neuvième à partir de la fin jusqu'à au second à partir de la fin
<SessCaseInsensitive>	Lorsque ce paramètre a pour valeur True, SessField et SessSection (s'ils sont spécifiés) peuvent comporter des valeurs à casse mixte. **Remarque :** Cette option doit être évitée, dans la mesure où la correspondance insensible à la casse utilise davantage de ressources système que la correspondance sensible à la casse. Ce paramètre s'applique uniquement au nom de paramètre et non à la valeur de paramètre.
<TimeGradesEnabled>	Lorsqu'il est activé, ce paramètre permet d'attribuer un niveau à un hit pour l'une des caractéristiques suivantes : • Web Server Page Gen : correspond au temps que met le serveur Web pour charger la page. • Network Transit : mesure la vitesse du réseau en fonction du temps qu'a passé un paquet sur le réseau. • Round Trip : correspond au temps de déplacement d'un paquet du client vers le serveur Web.

Tableau 20. Paramètres d'analyse (suite)

Option de configuration	Description
<WSGenBreaks>	Correspond au temps que met le serveur Web pour charger la page. Paires nom-valeur délimitées par des virgules (`name:value`, `name:value`).
<NetworkTransitBreaks>	Mesure la vitesse du réseau en fonction du temps qu'a passé un paquet sur le réseau. Paires nom-valeur délimitées par des virgules (`name:value`, `name:value`).
<RoundTripBreaks>	Correspond au temps de déplacement d'un paquet du client vers le serveur Web. Paires nom-valeur délimitées par des virgules (`name:value`, `name:value`).
<SamplingEnabled>	L'échantillonnage de session, s'il est activé, indique le pourcentage des sessions à supprimer de la capture.
<SamplePercentage>	Pourcentage de trafic à enregistrer, si l'échantillonnage est activé.
<PrivacyEnabled>	Détermine si la confidentialité est activée.
<InflatePreserveResponseOnErr>	Sélectionnez cette option pour activer la fonction de décompression. Si une réponse possède un en-tête de codage de contenu dont la valeur est `deflate`, `gzip` ou `x-gzip`, son corps est alors susceptible d'être décompressé à partir de son état compressé. Lorsque la décompression échoue, un message est consigné dans le journal notice. Lorsque la décompression aboutit, la valeur de l'en-tête de codage de contenu est écrasée par le caractère X. Par exemple, la valeur du codage de contenu peut être `XXXX`.
<XforwardingEnable>	Lorsque ce paramètre a pour valeur `True`, la PCA est configurée pour analyser une zone `HTTP-X-FORWARDING` spécifiée. **Remarque :** Cette entrée n'est pas créée tant que X-forwarding n'est pas activé. Pour plus d'informations, voir «Console Web de la PCA - Onglet Pipeline», à la page 101.
<XforwardingField>	Lorsque `XforwardingEnable` a pour valeur `True`, cette zone identifie la zone `HTTP-X-FORWARDING`. Cette entrée n'est pas créée tant que X-forwarding n'est pas activé. Pour plus d'informations, voir «Console Web de la PCA - Onglet Pipeline», à la page 101.
</Parse>	
<LastWSDescription>	Lorsque `TimeGrades` est activé, ce paramètre correspond à la description à utiliser pour les temps WSGen qui dépassent le dernier délai défini par `WSGenBreaks`.

Tableau 20. Paramètres d'analyse (suite)

Option de configuration	Description
<LastNTDescription>	Lorsque TimeGrades est activé, ce paramètre correspond à la description à utiliser pour les délais de transit dans le réseau qui dépassent le dernier délai défini par NetworkTransitBreaks.
<LastRTDescription>	Lorsque TimeGrades est activé, ce paramètre correspond à la description à utiliser pour les temps d'aller-retour qui dépassent le dernier délai défini par RoundTripBreaks.
<DeflateEnabled>	Si ce paramètre a pour valeur True, la réponse de chaque hit est compressée (si elle ne l'est pas déjà) avant qu'elle soit envoyée à l'homologue de distribution. La valeur par défaut est False.
<HitArchiveEnabled>	Si ce paramètre a pour valeur True, tous les hits capturés sont également consignés dans un fichier archive (TLA) sur l'unité locale. Il est essentiellement destiné à l'identification et la résolution des incidents et ne concerne pas les circonstances normales d'utilisation. La valeur par défaut est False.
<HitArchiveDirectory>	Répertoire dans lequel les archives de hits sont consignées lorsque HitArchiveEnabled=True.
<HitArchiveRollSizeMBytes>	Indique la taille de fichier évolutif en mégaoctets ; la valeur par défaut est de 100 Mo.

<Failover>

Vous pouvez configurer les paramètres de basculement à l'aide de la section «Console Web de la PCA - Onglet Reprise», à la page 161.

Tableau 21. Paramètres de basculement

Option de configuration	Description
<Activé>	Si le basculement est activé, une machine hôte Passive Capture de sauvegarde (subordonnée) reprend le contrôle si la machine principale (maître) échoue.
<MasterAddress>	Adresse de la machine de reprise maître.
<MasterPort>	Port de la machine de reprise maître.
<SlaveAddress>	Adresse de la machine de reprise subordonnée.
<SlavePort>	Port de la machine de reprise subordonnée.
<HeartbeatInterval>	Indique le temps d'attente entre les pulsations.
<HeartbeatTimeout>	Indique le délai d'attente de Passive Capture avant que la réponse à une pulsation n'expire.

Tableau 21. Paramètres de basculement (suite)

Option de configuration	Description
`<TimeoutLimit>`	Indique le nombre de dépassements du délai d'attente consécutifs autorisés avant un basculement forcé.
`<AutoFailback>`	Transfère le contrôle (état actif) de la machine hôte subordonnée de Passive Capture vers la machine hôte maître une fois que cette dernière est prête à reprendre le contrôle.
`<FailbackDelay>`	Délai minimum (en secondes) avant d'effectuer une reprise par restauration automatique.
`<FailoverOnSvcRestart>`	Cette option détermine si une reprise est déclenchée lorsque les services de capture redémarrent sur le serveur IBM Tealeaf Passive Capture Application actif.
`<RemoteMonitors>`	
`<RemoteMonitor>`	Un contrôleur à distance est un ordinateur (représenté par un nom d'hôte ou une adresse IP) qui est autorisé à recevoir les informations concernant l'état de la reprise en envoyant des signaux de présence à une machine hôte de Passive Capture configurée pour la reprise.
`<Host>`	Nom d'hôte du contrôleur à distance.
`<CanControl>`	Si cette option est activée, le contrôleur à distance peut forcer un basculement ou une reprise par restauration.
`</RemoteMonitor/>`	
`</Failover>`	
`</Conf>`	

Chapitre 4. Configuration de Packet Forwarder

IBM Tealeaf Packet Forwarder peut être configuré par l'intermédiaire des fichiers de configuration stockés dans le répertoire d'installation.

Le scénario typique d'un site Web en nuage inclurait un équilibreur de charge élastique (ELB) pour distribuer le trafic Web vers un niveau pour le serveur Web attribué dynamiquement qui consiste en plusieurs instances de serveur Web. Chaque instance de Web-serveur aurait une Packet Forwarder est installé pour transmettre le trafic Web capturées à une centralisé CX PCA. CX PCA s'exécute sur une instance de machine virtuelle et traite le trafic Web. Une fois l'instance Web-serveur est correctement configurée, une instance de machine Amazon (AMI) est créé pour l'instance. L'AMI est alors dynamiquement à disposition pour fournir autant d'instances que nécessaire.

Remarque : Au moment de la publication de cette publication, le nombre maximal d'instances de serveur Web doit être connu. Le nombre d'instances de serveur Web est utilisé dans la configuration du transfert de paquet afin de déterminer le nombre maximal de connexions TCP actives qui peut se connecter au récepteur du socket PCA de destination.

Configuration d'un Packet Forwarder pour communiquer avec le logiciel CX PCA

Pour traiter le trafic Web dans un environnement basé sur le Web, un Packet Forwarder doit être configuré pour transmettre des données à un CX PCA central qui fonctionne sur une machine virtuelle.

Les conditions préalables suivantes doivent être satisfaites avant de configurer le logiciel Packet Forwarder.

- Toutes les opérations d'installation et de configuration doivent être effectuées à l'aide du compte utilisateur `root`. L'utilisation de la commande `sudo` peut ne pas fournir des droits d'accès suffisants pour autoriser les modifications des paramètres système et peut provoquer une installation incomplète ou incorrecte.
- Installez le logiciel Packet Forwarder. Pour plus d'informations, voir «Installation du produit Packet Forwarder», à la page 26.

Procédez comme suit pour configurer Packet Forwarder et CX PCA pour la communication dans votre environnement basé sur le Cloud.

1. localisez `/usr/local/ctccap/etc/fwdr-conf.xml` sur le serveur proxy de réserve ou sur le serveur Web virtuel qui héberge l'émetteur Packet Forwarder.
2. Sauvegardez le fichier de configuration existants en copiant `/usr/local/ctccap/etc/fwdr-conf.xml` dans un répertoire de sauvegarde. Si votre fichier de configuration est corrompu ou invalide, vous pouvez effectuer une restauration depuis votre sauvegarde ou créer un nouveau fichier de configuration provenant de `fwdr-conf-defaults.xml`. `fwdr-conf-defaults.xml` contient les paramètres de configuration par défaut pour Packet Forwarder.
3. Editez `/usr/local/ctccap/etc/fwdr-conf.xml`. Vous pouvez utiliser `vi` de l'éditeur ou dans un autre éditeur de texte pour éditer le fichier de configuration.

4. Localisez la balise <PrimaryInterface> et éditez le nom du dispositif NIC virtuel du Packet Forwarder. Le Packet Forwarder capture le trafic provenant du serveur Web. Pour la plupart des installations, eth0 est utilisé comme nom d'unité.
5. Modifiez les numéros de port pour refléter le trafic des ports qui sont utilisés pour votre serveur. La règle de filtrage du trafic de capture par défaut est définie pour écouter sur le port 80 et le trafic 443.

   Exemple de paramètres de port :

```
<ListenTos>
<ListenTo>
<Port>80</Port>
<Port>443</Port>
</ListenTo>
</ListenTos>
```

6. Localisez la balise Delivery et éditez la connexion au réseau de distribution pour Packet Forwarder. Cela connecte Packet Forwarder à l'instance de machine virtuelle CX PCA centralisée.

   Exemple de paramètres de connexion au réseau de distribution :

```
<Peers>
<Peer>
<Address>127.0.0.1</Address&gt;
<Port>1888</Port>
</Peer>
</Peers>
```

7. Localisez et éditez la balise <Address> et <Port> correspondant à l'adresse IP interne affecté et le port du CX PCA qui est installée sur la machine virtuelle.

   Exemple de paramètre pour l'adresse IP interne de la machine virtuelle CX PCA:

   Remarque : La balise <Port> définit le numéro de port de la connexion réseau de base. Il s'agit d'un numéro de port de base où est défini le bloc de numéros de port utilisé pour le nombre d'instances de serveur Web que vous pouvez mettre à disposition. Par exemple, si vous savez qu'il y aura un maximum de cinq instances de serveur Webs qui peuvent être mises à disposition dynamiquement, alors le bloc de ports utilisés commence par 1888. Dans cet exemple, les numéros de port 1888 à 1892 sont utilisés d'après le maximum de cinq instances.

```
<Peers>
<Peer>
<Address>127.0.0.1</Address>
<Port>1888</Port>
</Peer>
</Peers>
```

8. Localisez et éditez la balise <MaxRotatePeers> pour définir le nombre maximal d'instances de serveur Web pouvant être alloué dynamiquement. La valeur par défaut est définie sur 1 pour une seule instance de serveur Web lorsqu'il n'y a pas d'autres instances du Packet Forwarder utilisé au niveau du serveur Web.

   Remarque : Si vous affectez statistiquement un nombre fixe d'instances de serveur Web aux émetteurs de paquets associés, alors <MaxRotatePeers> reste défini sur la valeur par défaut de 1. Chaque émetteur de paquet doit être configuré avec un numéro de port unique pour identifier une connexion réseau unique à l'instance de machine virtuelle CX PCA centralisée. Les numéros de ports doivent être affectés en ordre séquentiel. Cette opération est requise par le récepteur de socket CX PCA lorsqu'il est configuré pour les

connexions réseau du Packet Forwarder. Si vous décidez de démarrer par le numéro de port 1888 pour le premier émetteur de paquet, alors en définir cinq correspondrait aux ports de 1888 à 1892.

9. Enregistrez vos modifications dans le fichier de configuration.
10. Vous devez configurer une instance de destinataire Packet Forwarder pour chaque instance d'émetteur Packet Forwarder déployée. Pour plus d'informations, voir «Configuration d'un destinataire Packet Forwarder et du logiciel CX PCA pour recevoir des paquets transférés».

Une fois Packet Forwarder en cours d'exécution, vous pouvez également effectuer les actions suivantes :

- Vérifiez le statut d'un Packet Forwarder, en exécutant `service pktfwdr status`.
- Arrêtez un Packet Forwarder, en exécutant `service pktfwdr stop`.
- Affichez les statistiques d'un Packet Forwarder, en exécutant `ctcstats -p`.

Configuration d'un destinataire Packet Forwarder et du logiciel CX PCA pour recevoir des paquets transférés

Pour traiter le trafic Web dans un environnement basé sur le Cloud, les instances de destinataires Packet Forwarder doivent être déployées sur le logiciel central basé sur le Cloud CX PCA qui fonctionne sur une machine virtuelle.

Pour chaque instance d'émetteur Packet Forwarder déployée, vous devez également déployer une instance de destinataire Packet Forwarder sur le serveur CX PCA. Pour plus d'informations sur l'installation d'un Packet Forwarder, see «Installation du produit Packet Forwarder», à la page 26.

Procédez comme suit pour configurer les paramètres d'un destinataire Packet Forwarder.

1. Connectez-vous à la console Web CX PCA. Voir «Connexion à la console Web de la PCA», à la page 54 pour en savoir plus.
2. Modifiez le nombre d'instances du processus pipelined dans l'onglet Pipeline comme vous le souhaitez. Selon que les règles de confidentialité CX PCA ont été appliqués, le nombre par défaut de CX PCA `pipelined` les processus est défini sur un. Cette opération peut être insuffisant et peut être augmentée pour gérer la charge de traitement. Ceci suppose que l'instance VM dispose de ressources suffisantes, telles que les coeurs de processeur suffisante pour prendre en charge l'augmentation.
3. Sauvegardez les modifications apportées au CX PCA, mais ne pas redémarrer le CX PCA à ce stade.
4. Modifiez le fichier de configuration de CX PCA `ctc-conf.xml`. Pour plus d'informations, voir «Fichier de configuration Passive Capture `ctc-conf.xml`», à la page 171.
5. Localisez la balise de section `Capture` dans le fichier de configuration et modifier le contenu de cette section pour :

```
<ListenerSocketEnabled>true</ListenerSocketEnabled>
<TransparentLoadBalancingEnabled>false</TransparentLoadBalancingEnabled>
<SslSessionInfoOnMemcachedServer>false</SslSessionInfoOnMemcachedServer>
```

   Remarque : Si CX PCA est configuré pour déchiffrer le trafic SSL à partir de Packet Forwarder, alors définissez `<SslSessionInfoOnMemcachedServer>` sur `true`.

6. Repérez les paramètres socket récepteur et modifiez les paramètres de votre environnement réseau.

   L'exemple suivant affiche les paramètres du destinataire de socket par défaut :

```
<Listener>
<Module>pktr</Module>
<Logfile>/var/log/tealeaf/listener.log</Logfile>
<BasePort>1888</BasePort>
<Instances>1</Instances>
<Options>
 <Option>
  <Value>-p</Value>
 </Option></Options>
</Listener>
```

   La balise `BasePort` définit le numéro de port de base utilisé par le Packet Forwarder ou les Packet Forwarders. Il doit s'agir du même numéro de port pour CX PCA pour capturer correctement le trafic provenant du Packet Forwarder ou des Packet Forwarders. Le paramètre par défaut consiste à utiliser un port de base 1888 et à ne recevoir que d'un seul Packet Forwarder.

   La balise `Instances` définit le nombre maximal des Packet Forwarders auxquels CX PCA va se connecter. Définissez cette valeur en fonction du nombre total ou maximal tel que défini par le nombre de Packet Forwarders déployés.

7. Enregistrez vos modifications dans `ctc-conf.xml`.
8. Démarrez CX PCA. Pour plus d'informations, voir «Démarrage de la PCA», à la page 30.
9. Une fois CX PCA redémarré, vous pouvez démarrer votre niveau de serveur Web et tout Packet Forwarder déployé. Exécutez `service pktfwdr start` pour démarrer le démon Packet Forwarder.

Une fois le destinataire Packet Forwarder receiver en cours d'exécution, vous pouvez également effectuer les actions suivantes :

- Vérifiez le statut d'un Packet Forwarder, en exécutant `service pktfwdr status`.
- Arrêtez un Packet Forwarder, en exécutant `service pktfwdr stop`.
- Affichez les statistiques d'un Packet Forwarder, en exécutant `ctcstats -p`.

Chapitre 5. Clés SSL

Pour déchiffrer les transmissions à l'aide du protocole SSL, les clés SSL utilisées dans le flux de transactions doivent être fournies avec IBM Tealeaf Application de capture passive CX. Passez en revue et suivez les instructions de cette section pour générer et exporter la clé privée utilisée par IBM Tealeaf Application de capture passive CX.

1. «Paramétrage des clés SSL chiffrées»
2. «Exportation la clé privée SSL», à la page 198
3. «Création d'un certificat autosigné», à la page 207

Paramétrage des clés SSL chiffrées

Pour déchiffrer les connexions SSL, les clients doivent fournir le logiciel Passive Capture avec des clés SSL valides.

Remarque : En général, les clés privées SSL sont fournies au format PEM et converties pour que la PCA puisse les utiliser. Avant de commencer, vérifiez que tous les fichiers PEM que vous souhaitez convertir ne contiennent que la clé privée RSA. Par exemple, ils ne doivent pas contenir les informations sur le certificat et les erreurs d'attribution.

- Les fichiers PEM contenant des données supplémentaires peuvent toujours être convertis et ajoutés à la PCA. Cependant, avec ces clés, la PCA ne déchiffre pas correctement le trafic des clés SSL et n'envoie pas de message d'erreur ou d'avertissement.

Cette section explique comment préparer vos clés SSL valides pour qu'elles puissent être utilisées correctement et ensuite comment les charger dans la PCA.

- Conversion automatique : vous pouvez autoriser la PCA à convertir automatiquement des fichiers PEM en texte brut en des clés PTL sur son serveur. Ces clés sont ensuite chargées automatiquement dans la PCA pour être utilisées. Pour découvrir les limitations existantes concernant ce processus, voir «Conversion automatique des clés SSL», à la page 194.
- Conversion manuelle : si vous voulez contrôler chaque étape du processus de conversion, vous pouvez suivre les instructions de conversion manuelle. Voir «Etapes pour convertir les clés SSL manuellement», à la page 195.

Présentation

Le logiciel ne charge pas la clé SSL directement. Au lieu de cela, il charge un fichier chiffré contenant la clé SSL et un ID de hachage propre à la machine.

- Le chiffrement empêche les accès non autorisés au contenu de la clé SSL. Le fichier est chiffré à l'aide de l'algorithme triple DES.
- Le hachage propre à la machine empêche le fichier chiffré d'être utilisé par une autre installation de Passive Capture.

  Remarque : Certaines données que l'on trouve uniquement dans les cartes d'interface réseau installées sur la machine hôte de la PCA et qui font partie du processus de création de clés PTL chiffrées sont intégrées dans la clé. Si vous ajoutez ou supprimez des cartes d'interface réseau ou déplacez la PCA sur une

autre machine avec des cartes différentes, vous devez recréer les clés PTL à l'aide des fichiers de clés PEM principaux et des instructions fournies.

Ce fichier est stocké sur le serveur de Passive Capture au format PTL propriétaire. Une fois le fichier chargé et configuré, les fichiers de clés SSL d'origine peuvent être effacés.

Conversion automatique des clés SSL

Remarque : Pour la conversion automatique, les clés SSL doivent être stockées dans le répertoire `capturekeys` sur le serveur de la PCA. Si vous voulez les stocker dans un autre répertoire ou effectuer d'autres modifications dans le processus de configuration, vous devez les convertir manuellement. Voir «Etapes pour convertir les clés SSL manuellement», à la page 195.

Conversion automatique des fichiers PEM en fichiers PTL sur le serveur de la PCA

Une fois que vous obtenez un fichier PEM, la PCA peut créer le fichier PTL dont vous avez besoin.

Remarque : Ce processus ne fonctionne que pour les fichiers PEM non protégés par un mot de passe.

1. Copiez le fichier PEM dans le répertoire suivant :

   ```
   /usr/local/ctccap/etc/capturekeys
   ```

   Remarque : Ainsi, le fichier PEM est effacé de ce répertoire. Assurez-vous d'en conserver une copie à un autre endroit.
2. Relancez le logiciel IBM Tealeaf Application de capture passive CX.
3. Pendant le démarrage, la PCA convertit automatiquement le fichier PEM en clé PTL. Imaginons par exemple que le fichier `myprivatekey.pem` crée une clé PTL intitulée `myprivatekey.ptl`.
   - Le fichier PEM (`myprivatekey.pem`) est effacé de ce répertoire.
4. Afin de vérifier que la clé PTL a correctement été chargée, reportez-vous au fichier journal de capture (`var/log/tealeaf/capture.log`). Si la clé PTL est correctement chargée, le journal contient un message ressemblant à :

   ```
   reassd[4681]: Autoloaded key file:
   /usr/local/ctccap/etc/capturekeys/myprivatekey.ptl
   ```

Remarque : Après avoir vérifié que la conversion a fonctionné, supprimez les fichiers PEM du répertoire `capturekeys`. Lorsque la PCA démarre ou redémarre, une recherche de fichiers est effectuée dans ce répertoire et ceux-ci sont à nouveau convertis.

Conversion d'une clé privée SSL au format PFX en PTL

Si vous disposez d'une clé privée au format PFX provenant d'une source inconnue, vous pouvez utiliser les commandes suivantes afin de la convertir en clé PTL pour que Tealeaf puisse l'utiliser :

1. Déchiffrez le fichier et renommez-le en fichier PEM en exécutant la commande suivante sur la machine hôte de Passive Capture :

   ```
   openssl pkcs12 -nodes -nocerts -in key1.pfx -out key1.pem
   ```

2. Lorsque le mot de passe d'importation vous est demandé, saisissez celui que vous avez utilisé lorsque vous avez exporté le certificat vers un fichier PFX. Vous devez recevoir le message suivant :

   ```
   MAC verified OK.
   ```

3. Pour valider le fichier créé à partir de la commande pkcs12 :

   ```
   openssl rsa -check -noout -in <private_key_filename>
   ```

Etapes pour convertir les clés SSL manuellement

Les sections suivantes expliquent les étapes à suivre pour convertir manuellement les certificats en clés que la PCA peut utiliser.

Chargement de la PCA avec des clés SSL

Dans cette section, vous apprendrez à charger la PCA avec des clés SSL.

Chargement de la PCA avec des fichiers de clés SSL

Afin de charger Passive Capture avec au moins une clé SSL :

1. Obtenez un fichier PEM pour chaque clé SSL. Normalement, vous exécutez cette étape sur le serveur Web contenant les clés SSL. Dans le logiciel Passive Capture, la clé SSL doit être au format PEM, c'est-à-dire que le nom du fichier doit définir par une extension .pem. Le fichier PEM est un fichier texte ASCII contenant la clé SSL chiffrée. Voici un exemple de clé SSL au format PEM :

   ```
   -----DEMARRAGE CLE PRIVEE RSA-----
   MII ... (lignes de codage)
   ....
   -----FIN CLE PRIVEE RSA-----
   ```

   Si le serveur Web ne stocke pas ses clés privées au format PEM, vous devez alors les exporter et les convertir au format PEM. Pour les procédures d'exportation, voir la section «Exportation la clé privée SSL», à la page 198.
2. Transférez les fichiers PEM dans le répertoire `/usr/local/ctccap/etc` sur la machine hôte de Passive Capture.
3. Connectez-vous à la machine hôte de Passive Capture en tant qu'utilisateur racine et allez dans le répertoire `/usr/local/ctccap/etc`.
4. Chiffrez les fichiers PEM afin de créer un fichier PTL.
   a. Utilisez la commande `tealeaf pem2ptl` pour créer les fichiers PTL pour un ou plusieurs fichier PEM. Par exemple, si vous disposez de deux fichiers PEM intitulés `server1.pem` et `server2.pem`, vous pouvez créer des fichiers PTL pour chacun d'eux à l'aide de la commande suivante :

      ```
      tealeaf pem2ptl server1.pem server2.pem
      ```

      Cette commande permet de créer des fichiers intitulés `server1.ptl` et `server2.ptl` dans le même répertoire que les fichiers PEM.
      - La commande `tealeaf pem2ptl` ne permet pas de créer des fichiers PTL déjà existants. Elle configure les paramètres de propriété et d'autorisations des fichiers PTL qui en résultent afin que seul l'utilisateur `ctccap` puisse y accéder.

   b. Si vous possédez une édition plus ancienne du pack `Tealeaf-pca` qui ne propose pas la commande `tealeaf pem2ptl`, utilisez, pour chaque fichier PEM que vous souhaitez chiffrer, les commandes suivantes, en remplaçant `server1.pem` par le nom de votre fichier PEM :

      ```
      /usr/local/ctccap/bin/tltenc -in server1.pem
      chmod u=rw,go= server1.ptl
      chown ctccap server1.ptl
      ```

Afin de convertir un grand nombre de fichiers PEM, utilisez les commandes ls et xargs pour les chiffrer. Vous devez taper la ligne de commande ci-dessous sur une seule ligne. Celle-ci utilise la commande ls pour créer une liste de noms de fichiers. La barre verticale autorise la commande xargs à utiliser cette liste et exécuter l'utilitaire tltenc en se servant de chaque nom figurant sur cette liste.

```
ls -1 server1.pem server2.pem server3.pem | xargs -L 1 -t \
/usr/local/ctccap/bin/tltenc -in
```

Après avoir exécuté la commande précédente, utilisez les commandes suivantes pour configurer les paramètres de propriété et d'autorisations de tous les fichiers PTL. Vous pouvez utiliser des caractères de remplacement en toute sécurité car les paramètres de propriété et d'autorisation sont les seuls dont la PCA a besoin pour accéder à tous les fichiers PTL.

```
chmod u=rw,go= *.ptl
chown ctccap *.ptl
```

5. Supprimez les fichiers PEM de la machine hôte de Passive Capture. Vérifiez que Passive Capture a correctement décodé les connexions SSL avant d'effacer les fichiers PEM.

Une fois les clés SSL chargées sur la machine hôte de Passive Capture et converties en fichiers PTL, configurez Passive Capture pour qu'il les utilise. Si vous devez configurer des fichiers PTL, utilisez l'onglet **Clés SSL** dans la console Web. Quand vous configurez des fichiers PTL, il peut être plus simple d'utiliser un éditeur de texte comme nano ou vi afin de modifier directement le fichier de configuration.

Chargement de la PCA avec la console Web

Pour utiliser l'onglet **Clés SSL** de la console Web :

1. Utilisez un navigateur Internet pour vous connecter à la console Web de Passive Capture.
2. Cliquez sur l'onglet **Clés SSL**.
3. Cliquez sur **Chargé** en haut de la page pour voir les clés SSL qui sont chargées.
4. Saisissez un libellé de clé HTTPS descriptif dans la zone **Libellé** .
5. Saisissez le chemin d'accès complet du fichier PTL dans la zone de nom de fichiers **Fichier de clés**. Par exemple : /usr/local/ctccap/etc/server1.ptl.
6. Cliquez sur **Ajouter**. L'entrée qui vient d'être ajoutée pour le fichier PTL s'affiche sur la page mise à jour.
7. Effectuez à nouveau les étapes 4 à 6 pour chaque fichier PTL que Passive Capture doit utiliser.
8. Cliquez sur **Enregistrer les modifications** pour enregistrer les fichiers PTL ajoutés au fichier de configuration. Le programme de capture redémarre et utilise les nouveaux fichiers PTL que vous avez ajoutés.
9. Si le programme ne parvient pas à démarrer, reportez-vous au fichier capture.log afin de comprendre pourquoi.

Ajout de fichiers PTL

Pour modifier le fichier de configuration afin d'ajouter des fichiers PTL :

1. Connectez-vous à la machine hôte de Passive Capture en tant qu'utilisateur racine et accédez au répertoire /usr/local/ctccap/etc.
2. Modifiez le fichier de configuration de Passive Capture ctc-conf.xml.
3. Recherchez la ligne suivante :

```
<CaptureKeys></CaptureKeys>
```

4. Si Passive Capture est déjà configuré avec des fichiers PTL, les balises `<CaptureKeys>` et `</CaptureKeys>` ne sont pas sur la même ligne.
5. Ajoutez une entrée `<CaptureKey>` pour chaque fichier PTL entre `<CaptureKeys>` et `</CaptureKeys>`. Vous devez fournir un intitulé et un chemin d'accès complet au fichier PTL pour chaque entrée. Par exemple, l'entrée `<CaptureKey>` d'un fichier PTL hypothétique intitulé `/usr/local/ctccap/etc/web1.ptl` ressemblerait à ça :

```
<CaptureKey>
        <Label>Web1 Key </Label>
        <PrivateKeyFile>/usr/local/ctccap/etc/web1.ptl</PrivateKeyFile>
</CaptureKey>
```

   Voici un exemple de deux entrées `<CaptureKey>` configurées sur une machine hôte de Passive Capture :

```
<CaptureKeys>
        <CaptureKey>
              <Label>Web1 Key </Label>
              <PrivateKeyFile>/usr/local/ctccap/etc/web1.ptl</PrivateKeyFile>
       </CaptureKey>
              <CaptureKey>
              <Label>Web2 Key </Label>
              <PrivateKeyFile>/usr/local/ctccap/etc/web2.ptl</PrivateKeyFile>
       </CaptureKey>
</CaptureKeys>
```

6. Enregistrez les modifications apportées sur le fichier de configuration et quittez l'éditeur.
7. Relancez les programmes de capture à l'aide des commandes suivantes :

```
Tealeaf stop capture
Tealeaf start capture
```

8. Si le programme ne parvient pas à démarrer, reportez-vous au fichier `capture.log` afin de comprendre pourquoi.
9. Utilisez un navigateur Web pour vous connecter à la console Web de Passive Capture et cliquez sur l'onglet Clés SSL pour voir les fichiers PTL que vous avez configurés.

Fichiers PTL chargés automatiquement

A l'aide de la console Web, vous pouvez charger automatiquement les certificats SSL au format texte brut `.pem` ou protégé par un mot de passe `.pfx`.

Remarque : Pour des raisons de sécurité, cette fonctionnalité n'est accessible que par le protocole SSL par un utilisateur authentifié. Si vous n'accédez pas à cette page avec `https`, vous ne pourrez voir que les clés PTL déjà existantes.

1. Ouvrez la console Web.
2. Cliquez sur l'onglet **Clés SSL**.
3. Cliquez sur le lien **Capturer les clés** en haut de la page.
4. La page suivante s'affiche :

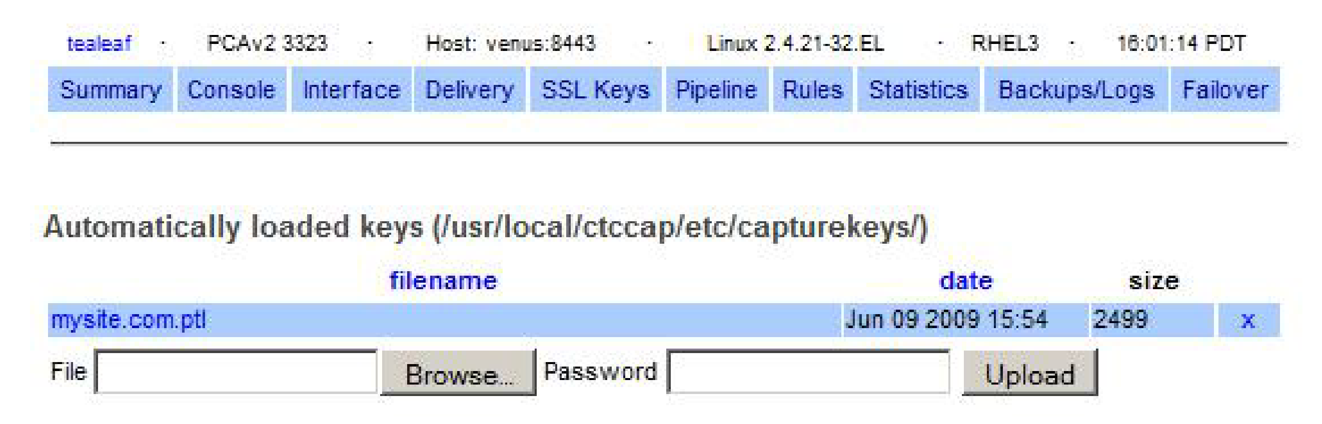


Figure 44. Chargement des clés

5. Pour sélectionner un fichier, cliquez sur **Parcourir...**.
6. Si la clé `.pem` est un fichier `.pfx` protégé par un mot de passe, saisissez le dans la zone **Mot de passe**.
   - S'il s'agit d'un fichier `.pem` en texte brut, ne saisissez rien dans la zone **Mot de passe**.
7. Pour convertir le certificat en clé, cliquez sur **Télécharger**.

Général

- Les clés converties sont stockées dans `/usr/local/ctccap/etc/capturekeys`.
- Les fichiers PEM ou PFX chargés qui représentent des clés valides sont convertis au format PTL.
- Le contenu des fichiers compressés téléchargés contenant des fichiers PEM valides est converti au format PTL.
- Dès qu'une conversion est finie, tous les fichiers qui ne sont pas au format PTL sont supprimés de `/usr/local/ctccap/etc/capturekeys`.
- Après avoir chargé les fichiers nécessaires, vous devez redémarrer la PCA sur l'onglet Console.

PFX

- Les clés protégées par un mot de passe (PFX) ne sont converties que si le mot de passe correspondant est fourni.
- Les clés protégées par un mot de passe sont directement converties en fichiers PTL.

PEM

- Les fichiers compressés ne doivent pas se trouver dans une hiérarchie (pas de répertoires).
- Les fichiers compressés ne peuvent contenir que des fichiers PEM.

Exportation la clé privée SSL

Dans l'éventualité où le trafic de l'application Web est transmis via HTTPS, le logiciel Passive Capture doit être configuré afin de déchiffrer les connexions SSL. Afin de réaliser cette configuration, il faut exporter une copie de la clé privée à partir d'un serveur Web existant vers Passive Capture.

Remarque : Ces instructions sont fournies pour l'exportation des clés privées à partir des systèmes tiers dont Tealeaf ne fait pas partie. Ces informations ne sont

fournies qu'à titre de référence et ne sont pas prises en charge par Tealeaf. Tealeaf se dégage de toute responsabilité les concernant. Consultez la documentation fournie avec votre serveur Web.

Pour plus d'informations sur la conversion des clés SSL pour que la PCA puisse les utiliser, voir «Paramétrage des clés SSL chiffrées», à la page 193.

Microsoft IIS 5 et 6

Vous trouverez dans les instructions suivantes les étapes à suivre pour exporter la clé privée de IIS au format PKCS #12 (`*.pfx`), à l'aide de l'assistant d'exportation du certificat de Microsoft IIS.

- Pour savoir comment convertir un fichier PFX à partir d'une source différente de IIS, voir «Paramétrage des clés SSL chiffrées», à la page 193.

1. Démarrez le gestionnaire de services Internet.
2. Sur le panneau de gauche, cliquez sur le dossier Sites Web qui se trouve sous le nom de la machine locale.
3. Sur le panneau de droite, faites un clic droit sur **Site Web par défaut** et sélectionnez **Propriétés**.
4. Cliquez sur l'onglet Sécurité du répertoire.
5. Cliquez sur **Afficher le certificat** pour voir le certificat.
6. Cliquez sur l'onglet Détails.
7. Cliquez sur **Copiez dans le fichier...**. L'assistant d'exportation du certificat se lance.
8. Cliquez sur **Suivant**. La fenêtre d'exportation des clés privées apparaît.
9. Sélectionnez le bouton d'option `Yes, export the private key` puis cliquez sur **Suivant**. La fenêtre du format du fichier d'exportation apparaît.
10. Sélectionnez le bouton d'option `Personal Information Exchange - PKCS #12 (.PFX)`. Sélectionnez `Enable strong protection` et `Include all certificates in the certificate path if possible`. Cliquez sur **Suivant**. La fenêtre du mot de passe apparaît.
11. Saisissez le mot de passe si nécessaire. Si le système est configuré pour demander un mot de passe, celui-ci permet un accès protégé au fichier.
12. Cliquez sur **Suivant**. La fenêtre du fichier à exporter apparaît.
13. Saisissez le nom du fichier ou parcourez les dossiers pour y accéder puis cliquez sur le bouton **Suivant**. La fenêtre de fin de l'assistant d'exportation de certificat apparaît.
14. Cliquez sur le bouton **Terminer**. Le certificat est exporté dans le fichier et un message de réussite s'affiche.
15. Copiez le fichier sur la machine hôte de Tealeaf Passive Capture. Assurez-vous que son nom est assez descriptif pour le serveur Web d'où il a été exporté.
16. Déchiffrez le fichier et renommez-le en PEM sur la machine hôte de Passive Capture à l'aide de la commande suivante :
    ```
    openssl pkcs12 -nodes -nocerts -in key1.pfx -out key1.pem
    ```
17. Lorsque le mot de passe d'importation vous est demandé, saisissez celui que vous avez utilisé lorsque vous avez exporté le certificat vers un fichier PFX. Vous devriez recevoir le message suivant :
    ```
    MAC verified OK.
    ```
18. Pour valider le fichier qui résulte de la commande pkcs12 :
    ```
    openssl rsa -check -noout -in <private_key_filename>
    ```

Microsoft IIS 3.0 et 4.0

Les instructions suivantes décrivent les étapes à suivre pour exporter la clé privée à partir d'Microsoft IIS 3.0 ou 4.0.

1. Exportez un fichier de sauvegarde du certificat à partir du gestionnaire de clés.
2. A partir du menu Clé dans le gestionnaire de clés, sélectionnez **Exporter la clé** puis **Fichier de sauvegarde**.
3. Après avoir lu les avertissements concernant le téléchargement d'informations sensibles sur votre disque dur, cliquez sur **OK**.
4. Entrez le nom de clé dans la case **Nom de fichier** et cliquez sur **Enregistrer**. Le fichier obtient une extension `*.KEY` et est enregistré sur un disque de 3,5 pouces sur le lecteur A: ou sur votre lecteur de disque dur.
5. Transférez le fichier de clés dans le répertoire `/usr/local/ctccap/etc` sur la machine hôte de Passive Capture.
6. Connectez-vous à la machine hôte de Passive Capture en tant qu'utilisateur racine.
7. Exécutez les commandes suivantes pour générer un fichier PEM à partir du fichier de clés IIS. Si la clé privée est protégée par un mot de passe, vous pouvez être invité à en saisir un. Les commandes suivantes utilisent plusieurs noms de fichiers comme par exemple :

   ```
   cd /usr/local/ctccap/etc
   ./sbin/iis-extract-net-key.pl iis.key > iis-net.key
   ./bin/openssl rsa -inform NET -in iis-net.key -out iis.pem
   ```

   `iis.key`: le fichier de clés IIS exporté à partir du serveur Web d'IIS et transféré sur la machine hôte de Passive Capture
   `iis-net.key`: portion de iis.key au format NET
   `iis.pem`: clé résultante, au format PEM
8. Validez le fichier à l'aide d'OpenSSL :

   ```
   ../bin/openssl rsa -check -noout -in iis.pem
   ```
9. Validez le résultat :
   Si celui-ci affiche `RSA key OK`, alors la clé a été correctement convertie.
   S'il affiche `Enter pass phrase for iis.pem`, alors la clé est chiffrée.
   Si le résultat affiche un autre message ou alors un message d'erreur, dans ce cas, soit le fichier est dans un mauvais format, soit il ne s'agit pas d'une clé.
10. Avec un fichier PEM valide, vous pouvez désormais supprimer les fichiers de clés IIS.

SunOne (iPlanet) 6.0

Les instructions suivantes permettent d'exporter la clé privée à partir de SunOne 6.0 :

Remarque : Pour effectuer cette procédure, OpenSSL doit être installé sur le serveur Web duquel la clé a été extraite.

1. Procurez-vous la base de données du certificat ainsi que celle de la clé pour l'instance dont vous voulez extraire la clé. Elles sont généralement disponibles dans `SERVER_ROOT/alias`.
2. Ajoutez à la variable PATH le texte suivant :

   ```
   SERVER_ROOT/bin/https/admin/bin
   ```
3. Ajoutez à la variable LD_LIBRARY_PATH le texte suivant :

   ```
   SERVER_ROOT/bin/https/lib:$\{LD_LIBRARY_PATH\}
   ```

4. Exportez le chemin d'accès ; LD_LIBRARY_PATH
5. Cet utilitaire pk12util permet d'exporter le certificat à partir de la base de données au format de la clé. Pendant que vous exportez la clé, vous êtes invité à saisir le mot de passe de celle-ci. Exécutez pk12util avec l'option suivante :

   ```
   pk12util -o <export filename> -n <cert filename> -d <certdir> -P <db \
   filename prefix for Sun DS>
   ```

   Remarque :

   `-o` - nom du fichier vers lequel le certificat est exporté.

   `-d` - option utilisée pour préciser l'emplacement du répertoire des certificats (le chemin d'accès à `cert8.db/key3.db`)

   `-P` - option utilisée pour préciser le nom du préfixe de la base de données (facultatif)

   Exemples :

   ```
   pk12util -o myCert.pk12 -n webServer.cert -d /sun/alias
   pk12util -o myCert.pk12 -n webServer.cert -d /sun/alias -P "https-hostname-"
   ```
6. A l'aide d'Open SSL, convertissez ce fichier au format PEM requis en utilisant l'option suivante :

   ```
   openssl pkcs12 -nodes -nocerts -in {Certname} -out https-{webinstance}.pem
   ```

   Remarque :

   `-in` - option utilisée pour préciser le fichier binaire d'entrée qui est aussi le fichier que vous avez défini comme le fichier de sortie avec l'option `-d` dans l'étape 4.

   `-out` - option utilisée pour préciser le fichier ASCII de sortie.

Traitement des anomalies d'iPlanet 6.0

Si vous rencontrez l'erreur DLL qui indique `pk12util: find cert by nickname failed: Failure to load dynamic library`, procédez alors comme suit :

1. Exécutez la commande suivante :

   ```
   wib@<servername>$ ldd pk12util
   ```
2. Copiez les fichiers suivants dans le répertoire `/usr/lib` :

   Fichier Emplacement source

   libssl3.so
   /opt/netsite/SunOne6.1/bin/https/lib/libssl3.so

   libsmime3.so
   /opt/netsite/SunOne6.1/bin/https/lib/libsmime3.so

   libnss3.so
   /opt/netsite/SunOne6.1/bin/https/lib/libnss3.so

   libplc4.so
   /opt/netsite/SunOne6.1/bin/https/lib/libplc4.so

   libplds4.so
   /opt/netsite/SunOne6.1/bin/https/lib/libplds4.so

   libnspr4.so
   /opt/netsite/SunOne6.1/bin/https/lib/libnspr4.so

libthread.so.1
: /usr/lib/libthread.so.1

libnsl.so.1
: /usr/lib/libnsl.so.1

libsocket.so.1
: /usr/lib/libsocket.so.1

librt.so.1
: /usr/lib/librt.so.1

libdl.so.1
: /usr/lib/libdl.so.1

libc.so.1
: /usr/lib/libc.so.1

libpthread.so.1
: /usr/lib/libpthread.so.1

libmp.so.2
: /usr/lib/libmp.so.2

libaio.so.1
: /usr/lib/libaio.so.1

libnspr_flt4.so
: /opt/netsite/SunOne6.1/bin/https/lib/cpu/sparcv8plus/libnspr_flt4.so

libc_psr.so.1
: /usr/platform/SUNW,Sun-Fire-480R/lib/libc_psr.so.1

3. Copiez les bases de données du certificat et de la clé dans un répertoire. Ensuite, effectuez la manoeuvre suivante sur ce répertoire pour vérifier son nom :

```
ls -la
/opt/netsite/SunOne6.1/alias
```

   - Voici la sortie qui en résulte :

```
drwxr-xr-x 3 wib webmaster 1024 Feb 15 11:26 .
drwxr-xr-x 15 wib webmaster 1024 Nov 26 23:25 ..
drwxr-xr-x 7 wib webmaster 1024 Dec 7 12:53 certs
-rwxr-xr-x 1 wib webmaster 2481 Feb 15 07:40 gte.pem
-rwxr-xr-x 1 wib webmaster 212992 Feb 15 12:52
   https-<www.company.com>-<servername>-cert8.db
-rwxr-xr-x 1 wib webmaster 65536 Feb 15 12:52
   https-<www.company.com>-<servername>-key3.db
-rwxr-xr-x 1 wib webmaster 32768 Feb 15 07:40 secmod.db
```

4. Exécutez la commande suivante : `pk12util`. Entrez le nom complet du certificat dans l'option `-P`, y compris le nom du serveur et le tiret (-) à la fin du nom du fichier (tout ce qui se trouve avant cert8 ou key3):

```
pk12util -o https-sunone.<URL> -n Server-Cert \
-d /opt/netsite/SunOne6.1/alias -P https-<www.company.com>-<servername>\-
```

5. Un nouveau fichier avec un nom de domaine sans extension est créé dans le répertoire et défini dans l'option `-d`.

Sun iPlanet 4.x

Les instructions suivantes expliquent comment exporter la clé privée à partir de la version 4 de Sun iPlanet.

1. Connectez-vous au serveur Web en tant qu'utilisateur racine.
2. Copiez le certificat et la clé d'iPlanet.
   a. Les fichiers d'instance d'iPlanet se trouvent dans `/apps/netscape/server4/alias/`.
   b. Copiez le fichier https-name**Key3.db d'instance d'iPlanet dans `/.netscape/key3.db`.
   c. Copiez le fichier https-name-*cert7.db d'instance d'iPlanet dans `/.netscape/cert7.db`.
3. Copiez le fichier secmod.db d'instance d'iPlanet dans `/.netscape/secmodule.db`.
4. Configurez X-display sur le bureau.
5. Lancez le navigateur Netscape à partir du serveur Web (`/opt/netscape/netscape`).
6. Cliquez sur l'icône de verrouillage **Sécurité**.
7. Dans la boîte de dialogue, cliquez sur **Certificats**, puis sur **Les vôtres** (comme indiqué dans l'image suivante).

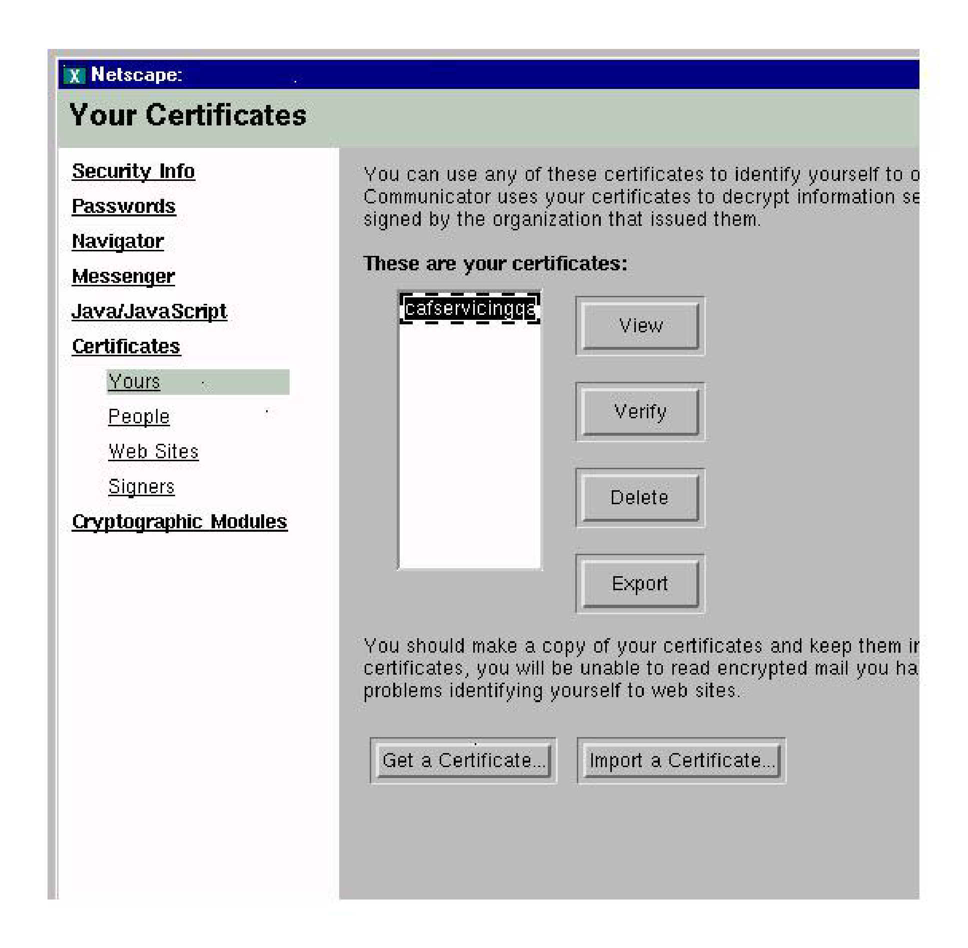


Figure 45. - Vos Certificats

8. Cliquez sur votre certificat puis sur **Exporter**. Le nom par défaut est le suivant : `Server-Cert`.
9. Saisissez le mot de passe pour le fichier de base de données de clé privée.
10. Saisissez un mot de passe pour protéger le fichier exporté.
11. Enregistrez le fichier exporté dans `/.netscape/xxxxx.p12`, où `xxxxx` correspond au nom du fichier.
12. Fermez le navigateur Netscape.

Apache 1.3.x, 2.0.x

Les instructions suivantes expliquent comment exporter la clé privée depuis les versions 1.3.x et 2.0.x d'Apache.

Remarque : Pour effectuer cette procédure, OpenSSL doit être installé sur le serveur Web duquel la clé a été extraite.

1. Si la clé est chiffrée, convertissez-la en clé non chiffrée. Pour cela, il faut effectuer la commande de base suivante :

   ```
   openssl rsa -in <old_private_key_filename> -out <new_private_key_filename>
   ```

   Remarque : Pour effectuer cette conversion, il vous faut un mot de passe.
2. Extrayez la clé du répertoire `/etc/httpd/conf/ssl.key`.

3. Renommez le fichier afin d'avoir une extension .pem.
4. Validez le fichier à l'aide d'OpenSSL :

```
openssl rsa -check -noout -in <private_key_filename>
```

5. Validez le résultat : si celui-ci affiche RSA key ok, alors la clé a été correctement exportée.
   S'il affiche Enter pass phrase for <private_key_filename>, alors il s'agit d'une clé, mais celle-ci est chiffrée.
   Si le résultat affiche un autre message ou alors un message d'erreur, dans ce cas, soit le fichier est dans un mauvais format, soit il ne s'agit pas d'une clé.

IBM HTTP Server

Les instructions suivantes expliquent comment exporter la clé privée à partir d'IBM HTTP Server.

1. Dans iKeyMan, sélectionnez le certificat, puis accédez à **Fichier** > **Exporter**.
2. Enregistrez le fichier avec l'extension PFX, attribuez-lui un mot de passe et sélectionnez l'option de chiffrement faible.
3. Transférez le fichier (en mode binaire) vers la machine hôte de Passive Capture.
4. Connectez-vous à la machine hôte de Passive Capture en tant qu'utilisateur racine. Exécutez la commande suivante :

```
openssl pkcs12 -nodes -nocerts -in x.pfx -out x.pem
```

5. Saisissez le mot de passe que vous avez défini lorsque vous avez exporté le fichier.
6. Validez le fichier à l'aide d'OpenSSL :

```
openssl rsa -check -noout -in key1.pem
```

7. Validez le résultat :
   Si celui-ci affiche RSA key ok, alors la clé a été correctement exportée.
   S'il affiche Enter pass phrase for <private_key_filename>, alors il s'agit d'une clé, mais celle-ci est chiffrée.
   Si le résultat affiche un autre message ou alors un message d'erreur, dans ce cas, soit le fichier est dans un mauvais format, soit il ne s'agit pas d'une clé.

Exportation à partir d'un magasin de clés Java (JKS)

Le magasin de clés Java™ (JKS) est l'implémentation par défaut pour la gestion des certificats et des clés dans les applications Java. Pour des raisons de sécurité, aucune méthode simple n'est fournie pour l'extraction de la clé privée à partir du magasin de clés.

Un cas de figure d'exportation classique est d'utiliser la clé dans un serveur Web Apache avec la norme PEM.

- Si le magasin de clés est configuré pour utiliser Openssl afin de créer votre certificat numérique, la clé privée sera alors disponible de manière transparente.
- Cependant, si vous utilisez iKeyman (IHS) ou alors l'outil de clé de Java, les fonctions d'exportation de clés privées ne sont pas fournies, pour des raisons de sécurité.
  - Il existe une solution de contournement connue permettant l'exportation à partir de l'outil de clé. Voir «Solution de contournement de l'outil de clé de Java», à la page 206.

La clé privée est nécessaire pour la conversion au format PKC12 d'un certificat signé au format DER reçu d'une autorité de certificat et que Tealeaf pourra utiliser.

En créant le certificat d'origine à l'aide d'iKeyman, vous pouvez recevoir le certificat signé d'une autorité de certificat.

- iKeyman peut recevoir un certificat au format DER binaire ou au format codé base-64.
- iKeyman peut importer à partir des formats CMS, JKS, JCEKS ou PKCS12.

  Remarque : L'extraction à partir d'environnements IBM HTTP Server nécessite une étape supplémentaire d'enregistrement de la base de données CMS au format JKS à l'aide d'iKeyman. Après conversion, l'extraction fonctionne comme si la base de données était format natif JKS.

Les clés PEM peuvent alors être exportées au format DER, celui-ci pouvant être utilisé par Apache. Pour exporter la clé privée à partir du format JKS, vous devez trouver et compiler la solution source de Java.

- Pour voir un exemple, rendez-vous sur `http://se9.blogspot.com/2008/10/extracting-private-key-from-java.html`.
- Plusieurs autres méthodes sont détaillées sur Internet.

Pour examiner une clé PEM au format DER, utilisez les commandes suivantes :

- Pour un certificat reçu d'une autorité de certificat :

  ```
  openssl x509 -noout -text -in CRT.der
  ```

- Pour une clé privée RSA :

  ```
  openssl rsa -noout -text -in rsa.key
  ```

Solution de contournement de l'outil de clé de Java

Par défaut, l'outil de clé de Java ne propose pas de moyens directs pour exporter la clé privée. Cependant, si votre version de l'utilitaire prend en charge l'exportation d'un magasin de clés JKS vers un autre format de magasin de clés, vous pouvez alors appliquer la solution de contournement suivante.

- Si votre outil de clés ne prend pas en charge cette exportation de magasin de clés, les méthodes de la section précédente peuvent alors s'appliquer.

Pour exporter à l'aide de l'outil de clé de Java :
L'exemple suivant illustre l'exportation d'un magasin de clés JKS vers pkcs12, un format que Tealeaf peut utiliser.

1. Exportez le magasin de clés vers un autre magasin de clés. Dans l'exemple suivant, le magasin de clés est exporté au format pkcs12 à l'aide d'une seule commande :

   ```
   keytool -importkeystore -srckeystore test-app.keystore
   -destkeystore mystore.p12 -srcstoretype JKS -deststoretype PKCS12
   -srcstorepass test-app-pwd -deststorepass test-app-pwd
   -srcalias test-app -destalias test-app -srckeypass test-app-pwd
   -destkeypass test-app-pwd-noprompt
   ```

   où :

   - `test-app.keystore` = chemin d'accès au magasin de clés de l'application
   - `mystore.p12` = chemin d'accès au magasin de clés pkcs12 cible
   - `JKS` = type de magasin de clés source. Il doit être paramétré sur `JKS`.
   - `PKCS12` = type de magasin de clés cible. Il doit être paramétré sur `PKCS12` lors de l'exportation vers pkcs12.
   - `test-app-pwd` = mot de passe d'accès au magasin de clés pouvant servir à la fois pour le magasin de clés et la clé sources, ainsi que pour le magasin de clés et la clé cibles.

- test-app = alias pour le magasin de clés qui peut être le même pour la source et la cible.

2. Lorsque le magasin de clés est exporté vers PKCS12, il vous faut utiliser openssl pour exporter la clé privée à partir d'un fichier de clés pkcs12 formaté :

```
openssl pkcs12 -in mystore.p12 -out mystore.pem \
-passin pass:test-app-pwd -passout pass:test-app-pwd
```

3. La clé privée protégée par un mot de passe se trouve désormais dans mystore.pem.
4. Tealeaf peut alors utiliser la clé privée.
   - Pour plus d'informations sur la validation des clés PEM, voir «Création d'un certificat autosigné».
   - Pour plus d'informations sur l'importation des clés, voir «Paramétrage des clés SSL chiffrées», à la page 193.

Création d'un certificat autosigné

Pour créer un certificat autosigné, vous devez utiliser l'utilitaire openssl pour créer une clé privée et un certificat autosigné pour cette clé. Le pack Tealeaf-pca fournit l'utilitaire openssl dans le répertoire/usr/local/ctccap/bin.

Pour suivre les instructions ci-dessous, vous devez être connecté à la machine hôte de Passive Capture en tant qu'utilisateur racine. Pour créer un certificat autosigné :

1. Générez la clé privée. L'exemple suivant permet de générer un fichier de clés RSA 2048 bits intitulé example.key:

```
/usr/local/ctccap/bin/openssl genrsa -out example.key 2048
```

2. Créez le certificat autosigné. L'exemple suivant permet de créer un fichier de certificat autosigné intitulé example.crt à l'aide du fichier de clés privées example.key créé dans l'étape 1. Avec l'option -days 365, le certificat est valide pendant une année entière :

```
/usr/local/ctccap/bin/openssl req -x509 -days 365 -newkey rsa:2048 -key \
  example.key -out example.crt
```

La commande openssl req demande plusieurs valeurs de manière interactive. Le tableau suivant affiche les invites et les exemples de réponses :

Invite Exemple de réponse

Nom du pays (code à deux lettres)
US

Nom de l'Etat ou de la province (nom complet)
California

Nom de la localité (une ville, par exemple)
San Francisco

Nom de l'organisation (une société, par exemple)
Tealeaf, une société d'IBM

Nom du subordonné de l'organisation (une section, par exemple)
Release Engineering

Nom usuel (VOTRE nom, par exemple)
pca.Tealeaf.com

Adresse e-mail
root@pca.Tealeaf.com

Le nom usuel doit correspondre au chemin d'accès DNS complet de la machine hôte de Passive Capture. Si la machine hôte n'a pas de nom DNS associé, utilisez alors l'adresse IP de l'ordinateur.

3. Maintenant, configurez les paramètres de propriété et d'autorisation corrects du fichier :
   a. Tous les fichiers de clés privées ne doivent être accessibles à la lecture qu'au compte utilisateur qui a besoin d'y accéder et de les lire. Les commandes `chmod` et `chown` ci-dessous permettent de configurer les paramètres de propriété et d'autorisation pour que seuls les processus de capture exécutés par l'utilisateur `ctccap` puissent accéder au fichier `example.key`:
      ```
      chmod go= example.key
      chown ctccap example.key
      ```
   b. Placez les fichiers dans un répertoire accessible au compte utilisateur. En ce qui concerne les fichiers de certificat et de clé utilisés par Passive Capture, placez-les dans le répertoire `/usr/local/ctccap/etc`.

Création du certificat autosigné à l'aide de l'algorithme SHA-2

La commande openssl utilise l'algorithme SHA-1 par défaut pour créer le certificat autosigné sur la PCA. Vous pouvez utiliser SHA-2 pour le hachage de signature numérique en ajoutant l'option `-sha256` comme dans l'exemple suivant, mais ceci n'est pas obligatoire :

Remarque : Les builds 3500 et plus récentes de la PCA prennent en charge cette commande.

```
/usr/local/ctccap/bin/openssl req -x509 -sha256 -days 365 -newkey rsa:2048 \
  -key example.key -out example.crt
```

Si vous n'utilisez pas la build 3500 ou une build ultérieure de la PCA, vous pouvez créer la clé SHA-2 sur un autre système Linux. Pour examiner les possibilités, exécutez la commande suivante dans un environnement ne contenant pas la PCA :

```
openssl dgst ?h
```

La sortie générée peut comprendre la ligne suivante :

```
-sha256         to use the sha256 message digest algorithm
```

Si la commande précédente s'affiche, alors l'installation Linuxaccepte l'option SHA-2. Vous pouvez exécuter la commande suivante sans fournir de chemin propre à la PCA :

```
openssl req -x509 -sha256 -days 365 -newkey rsa:2048 -key example.key -out \
  example.crt
```

Création d'une demande de certificat signé adressée à l'autorité de certificat interne

Si vous voulez utiliser votre propre autorité de certificat interne (CA) pour créer un certificat signé, procédez comme suit.

- Ces instructions utilisent l'utilitaire openssl comme exemple, mais d'autres utilitaires peuvent être utilisés.

1. Obtenez une clé privée RSA 2048 bits. Cette clé peut s'auto-générer de la manière suivante, en utilisant par défaut le chemin d'installation de la PCA pour accéder à la commande openssl de la PCA :
   ```
   /usr/local/ctccap/bin/openssl genrsa -out example.key 2048
   ```

2. Utilisez la clé privée RSA pour créer la demande de certificat signé (CSR). Si le fichier de clés correspond à `example.key`, alors la commande suivante permettra de créer un fichier CSR `cert_req.csr` :

   ```
   /usr/local/ctccap/bin/openssl req -new -key example.key -out cert_req.csr
   ```

   - Si, à la suite de cette commande, un message d'erreur mentionnant `openssl.cnf` apparaît, il faut alors configurer le chemin d'installation de la PCA permettant de placer le fichier `openssl.cnf` au bon endroit. Dans ce cas, vous pouvez appliquer l'option `-config` pour définir le nouveau chemin d'installation, différent de celui défini par défaut. Dans l'exemple qui suit, il s'agit du chemin `/opt/tealeaf`.

     ```
     /opt/tealeaf/bin/openssl req -new -config /opt/tealeaf/ssl/openssl.cnf -key \
       example.key -out cert_req.csr
     ```

3. Lors de la création du fichier CSR à l'aide de l'une des commandes précédentes, des valeurs vous sont demandées pour le certificat public. Pour plus d'informations concernant les valeurs à insérer, voir «Création d'un certificat autosigné», à la page 207.
4. Lorsque le fichier CSR est créé, l'autorité de certificat interne peut l'utiliser pour terminer le processus de création d'un certificat signé.
5. Le fichier du certificat signé peut désormais être appliqué de la même manière qu'un certificat auto-signé utilisable PCA.
   - Voir Chapitre 2, «Installation», à la page 17.

Scripts utilitaires

Le pack `Tealeaf-pca` fournit un script permettant de simplifier les étapes à suivre pour créer des certificats autosignés. Le chemin complet d'accès au fichier script est : `/usr/local/ctccap/sbin/gen-self-signed-cert.sh`. Définissez les noms des fichiers de la nouvelle clé privée et du certificat comme arguments pour `gen-self-signed-cert.sh`.

Le script crée un ficher de clés RSA 2048 bits ainsi qu'un certificat autosigné qui sont valides pendant 10 ans (3 650 jours). Les fichiers résultats appartiennent à l'utilisateur `ctccap` et seul ce dernier peut lire la clé privée. Voici un exemple de requête de ce script :

```
/usr/local/ctccap/sbin/gen-self-signed-cert.sh example.key example.crt
```

Le pack `Tealeaf-pca` crée le nombre de certificats autosignés dont vous avez besoin lorsque vous l'installez. Si vous modifiez le nom de la machine hôte de Passive Capture, vous pouvez recréer ces certificats. Pour recréer tous ces certificats, utilisez la commande suivante :

```
env FORCE=YES /usr/local/ctccap/sbin/all-self-signed-certs.sh
```

La commande précédente permet d'effacer et de recréer les fichiers suivants :

```
/usr/local/ctccap/etc/tealeaf-pca.crt
/usr/local/ctccap/etc/tealeaf-pca.key
/usr/local/ctccap/etc/tealeaf-tts.crt
/usr/local/ctccap/etc/tealeaf-tts.key
/usr/local/ctccap/etc/tealeaf-tts.pem
/usr/local/ctccap/etc/tealeaf-web.crt
/usr/local/ctccap/etc/tealeaf-web.key
```

Déploiement des certificats SSL utilisables par la console Web de la PCA

Vous pouvez déployer autant de certificats SSL personnalisés utilisables par la console Web de la PCA que nécessaire pour assurer un accès sécurisé à la console.

Remarque : Le niveau de chiffrement ainsi que d'autres caractéristiques relatives au certificat doivent être définies afin de répondre aux besoins de votre entreprise.

1. Obtenez ou créez le certificat SSL.
   - La PCA utilise le certificat autosigné et la clé fournis par défaut. Pour plus d'informations sur la création d'un certificat autosigné, voir «Création d'un certificat autosigné», à la page 207.
   - Tealeaf fournit un script utilitaire simplifiant le processus de création d'un certificat autosigné. Ce script crée un certificat à l'aide d'un ensemble réduit d'options de configuration. Voir «Scripts utilitaires», à la page 209.
2. Le certificat et le fichier de clés créés doivent être ajoutés au fichier de configuration d'Apache. Ce fichier est stocké à l'emplacement suivant :

   ```
   /usr/local/ctccap/etc/httpd.conf
   ```
3. Dans l'exemple suivant, le nom de fichier du certificat est `tealeaf-web.crt` et le nom de fichier de la clé est `tealeaf-web.key` :

   ```
   Define SSLCERTFILE ${SYSCONFDIR}/tealeaf-web.crt
   Define SSLKEYFILE ${SYSCONFDIR}/tealeaf-web.key
   ```
4. Enregistrez le fichier.
5. Redémarrez la PCA.
6. Tous les utilisateurs de la console Web doivent maintenant se connecter à l'aide du protocole SSL.
   - Pour plus d'informations sur la manière de se connecter à l'aide du protocole SSL, voir«Navigateurs pris en charge pour la console Web de la PCA», à la page 54.
   - Pour plus d'informations sur la modification des ports que la console Web de la PCA écoute, voir «Navigateurs pris en charge pour la console Web de la PCA», à la page 54.

Configuration du service de transport Tealeaf pour le chiffrement SSL

Pour chiffrer la communication entre la machine hôte de Passive Capture et le service de transport Tealeaf, vous devez obtenir un certificat SSL. Configurez ensuite le logiciel Passive Capture et le service de transport Tealeaf pour que celui-ci l'utilise.

- Le certificat doit être une clé privée 2048 bits.
- Le certificat est installé sur les machines de la PCA et du service de transport Tealeaf. La PCA a besoin du certificat pour démarrer, et le service de transport Tealeaf l'utilise pour gérer les connexions sécurisées avec la PCA.

  Remarque : Les transmissions entre la PCA et le service de transport Tealeaf via le protocole SSL nécessitent un traitement supplémentaire et peuvent affecter la capacité de traitement globale.

1. Obtenez le certificat SSL.
   - Si vous créez votre propre certificat autosigné, vous devez aussi créer une clé privée 2048 bits. Voir «Création d'un certificat autosigné», à la page 207.
   a. Le pack `Tealeaf-pca` crée un certificat autosigné à utiliser lorsque vous configurez le chiffrement SSL de la communication réseau entre la machine

hôte de Passive Capture et le service de transport Tealeaf. Ce certificat autosigné contient le nom de la machine hôte au moment de l'installation du pack.

b. Les fichiers de certificat et de clé suivants sont créés par le pack `Tealeaf-pca` :
   - `/usr/local/ctccap/etc/tealeaf-tts.crt` (fichier du certificat)
   - `/usr/local/ctccap/etc/tealeaf-tts.key` (fichier de clé)
   - `/usr/local/ctccap/etc/tealeaf-tts.pem` (fichiers de certificat et de clé combinés en un seul dans le système DOS EOL)

2. Vous pouvez choisir d'utiliser le fichier PEM ci-dessus ou alors créer votre propre fichier.
   a. Une fois les fichiers de certificat et de clé privée créés, utilisez le script `/usr/local/ctccap/bin/crlf.sh` pour créer un seul fichier ASCII DOS-EOL dont le service de transport Tealeaf a besoin : Par exemple, si votre clé privée se trouve dans le fichier `example.key` et votre certificat dans le fichier `example.crt`, utilisez alors la commande suivante pour créer un fichier DOS EOL unique intitulé `example.pem`

      ```
      /usr/local/ctccap/bin/crlf.sh example.key example.crt > example.pem
      ```

   b. Le fichier qui en résulte contient une clé privée, vous devez donc limiter ses paramètres de propriété et d'autorisation à l'aide des commandes `chmod` et `chown`.

3. Transférez le fichier PEM DOS EOL sur la machine qui exécute le service de transport Tealeaf. Dans l'idéal, vous devez limiter son accès au service de transport Transport uniquement.
   - Le certificat doit être installé sur le répertoire racine d'installation de Tealeaf.

4. Si besoin est, vous pouvez utiliser le lecteur d'archive de Tealeaf pour vérifier que le certificat est valide et utilisable. Voir «Test du certificat SSL utilisé par le service de transport», à la page 212.

5. Sur le serveur qui héberge le service de transport Tealeaf, modifiez le fichier `TealeafCaptureSocket.cfg`.
   - Vous pouvez aussi effectuer des modifications dans la configuration via Pipeline Editor dans TMS, un éditeur qui propose une gestion des versions et une affectation centralisées des fichiers de configuration de Tealeaf. Modifiez le fichier de configuration brut du service de transport et insérez-y les valeurs dans la section `[Globals]`. Voir "Onglet Vue globale de TMS" dans le manuel *IBM Tealeaf cxImpact - Guide d'administration*.

   a. Dans la section `[Globals]`, ajoutez ou modifiez les directives suivantes au chemin d'accès au fichier PEM. Si les fichiers ne se trouvent pas dans le répertoire d'installation de Tealeaf, précisez alors le chemin complet d'accès aux fichiers.

      ```
      CertificateFile=css-cert.pem
      PrivateKeyFile=css-cert.pem
      ```

   b. A l'aide du fichier `example.pem` de notre exemple, modifiez `css-cert.pem` pour obtenir le résultat suivant :

      ```
      CertificateFile=example.pem
      PrivateKeyFile=example.pem
      ```

   c. Dans la section `[Globals]`, insérez le numéro de port que le service de transport Tealeaf écoute afin de capter le trafic SSL. Insérez le code suivant :

      ```
      SSLPort=1967:DataDrop
      ```

- `1967` correspond au numéro du port que le service de transport Tealeaf écoute pour le trafic SSL. Il s'agit de la valeur par défaut. Vous pouvez la modifier si nécessaire.

  Remarque : Ce numéro de port ne doit pas être utilisé par un autre pipeline ou composant Tealeaf pour surveiller le trafic.
- `DataDrop` correspond à l'agent de session dans le pipeline configuré pour traiter le trafic SSL reçu.

6. Connectez-vous à l'interface utilisateur Web de configuration de Passive Capture et cliquez sur l'onglet **Distribution**. Voir «Console Web de la PCA - Onglet Distribution», à la page 92.
   a. Dans la section des destinataires cibles, cliquez sur **Ajouter**.
   b. La page Ajouter un destinataire pour la distribution des hits s'affiche. Saisissez l'adresse et le port de l'hôte dans les zones correspondantes, cochez la case **Sécuriser** puis cliquez sur **OK**.

      Remarque : Le port saisi doit correspondre au port d'écoute du trafic SSL sur le service de transport. Le port par défaut est le suivant : `1967`.
7. La page Ajouter un certificat pour une distribution sécurisée s'affiche. Collez le certificat et cliquez sur **OK** pour enregistrer les modifications. Le certificat correspond à la partie de texte ASCII qui commence par la ligne suivante :

   ```
   -----BEGIN CERTIFICATE-----
   ```

   et qui s'arrête après la ligne suivante :

   ```
   -----END CERTIFICATE-----
   ```
8. Copiez et collez tout ce qui se trouve entre la ligne `BEGIN` et la ligne `END` (y compris celles-ci).
9. Redémarrez la PCA.
10. Redémarrez le service de transport.

Test du certificat SSL utilisé par le service de transport

Avant de déployer le certificat SSL sur la machine qui héberge le service de transport Tealeaf, vérifiez que le certificat est valide et utilisable par le lecteur d'archive de Tealeaf.

1. Laissez le certificat SSL installé sur la PCA.
2. Dans le fichier `ArchiveReader.cfg` du répertoire d'installation de Tealeaf sur la machine hôte du service de transport Tealeaf, trouvez la section `[Socket]`.
3. Pour configurer le connecteur afin qu'il utilise le protocole SSL, saisissez ou paramétrez le code suivant :

   ```
   USESSL=True
   ```
4. Paramétrez le serveur pour qu'il soit en mode `localhost`.
5. Configurez les valeurs suivantes sur le nom de fichier du certificat installé dans le répertoire d'installation racine de Tealeaf. Retirez le signe dièse (#) avant la ligne de configuration pour l'activer.

   ```
   CertificateFile=css-cert.pem
   PrivateKeyFile=css-cert.pem
   ```
6. Enregistrez le fichier.
7. Utilisez le lecteur d'archive pour soumettre des hits au service de transport.
   - Voir "Lecteur d'archive de Tealeaf - Exécuter les sessions archivées" dans le manuel de configuration d'*IBM Tealeaf CX*.
8. Dans l'onglet Statut du pipeline TMS, vérifiez que les hits sont capturés et traités par le bon pipeline.

- Voir "Onglet Statut du pipeline TMS" dans le manuel *IBM Tealeaf cxImpact - Guide d'administration*.

9. Si les hits sont capturés et traités, alors le certificat SSL fonctionne correctement.
10. Vous pouvez maintenant appliquer les modifications apportées à la configuration à la section `[Globals]` du fichier `TealeafCaptureSocket.cfg`. Voir «Configuration du service de transport Tealeaf pour le chiffrement SSL», à la page 210.

Activation des statistiques PCA dans le statut de Tealeaf

Pour activer l'affichage des informations sur les statistiques de la PCA dans le rapport de statut de Tealeaf, vous devez créer une référence au serveur de l'application de capture à la page Gestion du portail.

- Dans le menu Portail, sélectionnez **Tealeaf** > **Gestion du portail**.
- Voir "Serveurs de gestion de Tealeaf" dans le manuel *IBM Tealeaf cxImpact - Guide d'administration* .

Suppression ou consultation du certificat

Si vous voulez supprimer ou consulter le certificat, procédez comme suit :

1. Démarrez Internet Explorer sur le poste de travail où l'utilitaire du statut du portail s'exécute.
2. Sélectionnez **Outils** > **Options Internet**.
3. Cliquez sur l'onglet **Contenu**.
4. Cliquez sur **Certificats**.
5. La fenêtre Certificats s'affiche. Cliquez sur l'onglet **Autorités de certification racines de confiance**.
6. Vous pouvez maintenant sélectionner le certificat à supprimer ou à consulter.

Validation des clés PEM

Pour valider le fichier à l'aide d'OpenSSL, utilisez la commande suivante :

```
/usr/local/ctccap/bin/openssl rsa -check -noout -in <filename>
```

Voici le format attendu :

```
-----BEGIN RSA PRIVATE KEY-----
.... (lignes de codage)
....
-----END RSA PRIVATE KEY-----
```

Chapitre 6. Mesure des performances

Le calcul des performances fournit des détails sur les mesures de performances et d'horodatage du logiciel Passive Capture.

- Les horodatages ne font pas partie du Datastream HTTP, c'est pourquoi la PCA doit les insérer comme partie intégrante de son processus de capture.

Présentation de l'horodatage

Passive Capture propose un ensemble varié de valeurs horaires disponibles à l'analyse.

Remarque : Ces informations sur l'horodatage ne sont pertinentes que pour les données capturées par Passive Capture. Elles ne reflètent aucun horodatage ou traitement effectué par un autre logiciel Tealeaf.

Hypothèses

Pour les hypothèses suivantes, il faut :

- Que tous les horodatages soient créés par Passive Capture au point de capture. Lorsque le fichier voit des données au point de capture, il leur attribue alors un horodatage.
- Qu'une faible distance, presque négligeable, sépare la machine hôte de Passive Capture de la source qui génère le protocole HTTP. Cependant, ce facteur ne doit pas avoir une incidence considérable sur les horodatages puisque les données passent sans interruption du serveur Web au client.
- Que les données soient envoyées aussi vite que le permet le chemin réseau de bout en bout. D'éventuelles anomalies peuvent avoir des répercussions sur la précision de l'horodatage du trafic qui arrive à la PCA. Si le point de capture correspond à un miroir de port de commutateur, les mémoires tampon internes utilisées pour rassembler le trafic miroir peuvent modifier l'heure d'arrivée de ses données en temps réel. Les mémoires tampon peuvent contenir et découper le trafic du miroir de port à tout moment, ce qui peuvent avoir des répercussions sur l'exactitude des données. D'autres périphériques réseau peuvent aussi modifier l'heure d'arrivée des données si celles-ci font partie du chemin du trafic de capture mais pas si elles font partie du chemin du trafic en temps réel.
- Que tous les horodatages soient indiqués en heure GMT avec une précision à la microseconde. Une microseconde correspond à un millionième de seconde.

Remarque : Les horodatages enregistrés par IBM Tealeaf Application de capture passive CX représentent les estimations les plus proches de la réalité. Dans l'installation d'IBM Tealeaf cxImpact par défaut, ces horodatages ne comprennent pas les informations de rendu du navigateur client. Lorsque Tealeaf UI Capture est installé et activé dans votre application Web, ces informations sont capturées et signalées par le biais du portail.

- Pour plus d'informations sur les notifications côté client, voir la section "Analyse des performances" dans le manuel de notification d'*IBM Tealeaf*.
- Le composant Tealeaf IBM Tealeaf Capture d'interface utilisateur CX pour AJAX n'est pas compris dans la licence de la plateforme d'IBM Tealeaf CX. Contactez votre interlocuteur IBM Tealeaf.

- Voir section "Guide UI Capture for Ajax" dans le manuel d'*IBM Tealeaf UI Capture for Ajax*.

Exemples d'horodatages dans la demande

Les valeurs suivantes s'affichent à titre d'exemple dans la demande une fois que la PCA a créé ses horodatages.

```
RequestTimeEx=2009-02-26T15:33:58.347692Z
RequestEndTimeEx=2009-02-26T15:33:58.347836Z
ResponseStartTimeEx=2009-02-26T15:33:58.352928Z
ResponseTimeEx=2009-02-26T15:33:58.552479Z
ResponseAckTimeEx=2009-02-26T15:33:58.693390Z
TLapiArrivalTimeEx=2009-02-26T15:33:58.676361Z
ReqTTLB=144
RspTTFB=5092
RspTTLB=199551
RspTTLA=140911
ConnSpeed=628604
ConnType=DSL
WS_Generation=5092
WS_Grade=ExcellentWS
WS_GradeEx=0
NT_Total=340462
NT_Grade=ExcellentNT
NT_GradeEx=0
RT_Total=345554
RT_Grade=ExcellentRT
RT_GradeEx=0
```

Eléments
Utilisation*

RequestEndTimeEx=2009-02-26T15:33:58.
ResponseStartTimeEx=2009-02-26T15:33:58.
ResponseAckTimeEx=2009-02-26T15:33:58.
WS_Generation=5092
NT_Total=340462
RT_Total=345554
Utilisés dans le calcul des horodatages et du comportement réseau

347836
352928
693390 Valeurs d'horodatage utilisées pour les calculs ultérieurs

Définitions et valeurs d'horodatage dans la demande

Le tableau ci-dessous explique chacune des valeurs qui se trouvent dans la section [timestamp] de la demande :

Valeur Description

RequestTimeEx
Début de la demande. Horodatage correspondant au moment où la PCA a vu le premier paquet de la demande.

RequestEndTimeEx
Fin de la demande. Horodatage correspondant au moment où la PCA a vu le dernier paquet de la demande.

ResponseStartTimeEx
: Début de la réponse. Horodatage correspondant au moment où la PCA a vu le premier paquet de la réponse. Si aucun paquet de réponse n'a été repéré, la valeur RequestEndTimeEx est alors utilisée.

ResponseTimeEx
: Fin de la réponse. Horodatage correspondant au moment où la PCA a vu le dernier paquet de la réponse. Si aucun paquet de réponse n'a été repéré, la valeur RequestEndTimeEx est alors utilisée.

ResponseAckTimeEx
: Horodatage correspondant au moment où la PCA a vu que le client/navigateur avait reconnu le dernier paquet de la réponse. Si aucun paquet de réponse n'a été repéré, la valeur RequestEndTimeEx est alors utilisée.

TLapiArrivalTimeEx
: Cet horodatage indique lorsqu'un hit arrive dans le processus pipelined de la PCA. Le réassemblage d'un hit peut finir bien plus tard si un hit incomplet a été réassemblé ou retardé en raison d'un paquet de données considérablement en retard. Dans un cas de figure normal, cet horodatage doit être le même que `ResponseTimeEx`. Une grande différence entre les deux valeurs peut indiquer une anomalie de réseau.

ReqTTLB
: Durée en microsecondes entre les arrivées du premier et du dernier paquets de la demande (`RequestEndTimeEx` moins `RequestTimeEx`). Cette valeur ne comprend pas l'heure réseau.

RspTTFB
: Durée (en microsecondes) entre le début de la demande et l'arrivée de la première page de réponse (`ResponseTimeStartEx` moins `RequestTimeEx`). Cette valeur représente en général une estimation précise de l'heure à laquelle le serveur Web a demandé la création de la page de réponse. En particulier, si la page entière est mise en mémoire tampon (cette action est effectuée par défaut dans les environnements ASP.NET et dans la plupart des environnements J2EE), ce calcul prédit alors de manière exacte la durée qu'il faudra à l'infrastructure côté serveur pour répondre.
: - Si le serveur Web a assemblé les données en blocs, cette valeur peut être inexacte.

RspTTLB
: Durée en microsecondes entre les arrivées du premier et du dernier paquets de la réponse (`ResponseTimeEx` moins `ResponseStartTimeEx`). Cette valeur ne comprend pas l'heure réseau.

RspTTLA
: Durée nécessaire à la reconnaissance par le client/navigateur du dernier paquet de données (`ResponseACKTimeEx` moins `ResponseTimeEx`). Cette valeur indique la durée nécessaire à l'aller-retour réseau.
: - Pour calculer la durée qu'il faut pour un aller simple, divisez cette valeur par 2.

ConnSpeed
: Vitesse de connexion, en bits par seconde (bps). Cette valeur est calculée en divisant la taille moyenne de la réponse par la durée moyenne qu'il lui faut pour être distribuée.
: - Lorsque la vitesse de connexion est en cours de calcul, tous les événements relatifs à l'interface client sont ignorés.

ConnType
Fondée sur le paramètre ConnSpeed, cette valeur est définie sur `Dialup`, `ISDN`, `DSL` ou `T1`.

WS_Generation
Durée en microsecondes nécessaire au serveur Web pour créer la réponse. Cette valeur est obtenue par le calcul suivant : `ResponseStartTimeEx - RequestEndTimeEx`

- Voir «Durée de création d'une page», à la page 221.

WS_Grade
Niveau attribué à la durée nécessaire au serveur Web pour créer une page (`WS_Generation`). Les valeurs possibles sont les suivantes : `ExcellentWS`, `Very GoodWS`, `GoodWS`, `FairWS`, `PoorWS` ou `IncompleteWS`.

- Cette valeur est indexée par défaut.

WS_GradeEx
Nombre entre `0` et `4` représentant le groupement d'intervalles TimeGrades pour la durée nécessaire au serveur Web pour créer une page. Voir «Console Web de la PCA - Onglet Pipeline», à la page 101.

NT_Total
Durée du déplacement réseau en microsecondes.

- Voir «Durée réseau», à la page 221.

NT_Grade
Niveau attribué à la durée du déplacement réseau (`NT_Total`). Les valeurs possibles sont les suivantes : `ExcellentNT`, `Very GoodNT`, `GoodNT`, `FairNT`, `PoorNT` ou `IncompleteNT`.

- Cette valeur est indexée par défaut.

NT_GradeEx
Nombre entre `0` et `4` représentant le groupement d'intervalles TimeGrades pour la durée du déplacement réseau. Voir «Console Web de la PCA - Onglet Pipeline», à la page 101.

RT_Total
Durée totale du déplacement aller-retour en microsecondes.

RT_Grade
Niveau global des performances réseau. Les valeurs possibles sont les suivantes : `ExcellentRT`, `Very GoodRT`, `GoodRT`, `FairRT`, `PoorRT` ou `IncompleteRT`.

- Cette valeur est indexée par défaut.

RT_GradeEx
Nombre entre `0` et `4` représentant le groupement d'intervalles TimeGrades pour la durée du déplacement réseau aller-retour. Voir «Console Web de la PCA - Onglet Pipeline», à la page 101.

Calcul de durées à partir des horodatages

Pour déterminer les performances, voici les trois horodatages les plus importants de la demande :

- `RequestTimeEx`
- `ResponseStartTimeEx`
- `ResponseAckTimeEx`

1. La première valeur temporelle en microsecondes correspond à la différence entre le moment où la PCA voit la fin de la demande et celui où la réponse commence : `RspTTFB = ResponseStartTimeEx - RequestTimeEx`
2. La deuxième valeur temporelle en microsecondes correspond à la différence entre le moment où la PCA voit la fin de la demande et celui où la réponse se termine : `RspTTLB = ResponseTimeEx - ResponseStartTimeEx`
3. La troisième valeur temporelle en microsecondes correspond à la durée nécessaire à la dernière réponse pour se déplacer de la PCA au visiteur. Durée nécessaire à la demande initiale pour aller de l'utilisateur à la PCA, ce qui correspond au calcul de la durée nécessaire à l'aller-retour réseau : `RspTTLA = ResponseACKTimeEx` minus `ResponseTimeEx`

Facteurs ayant des répercussions sur les valeurs d'horodatage

Pour évaluer les horodatages, les facteurs suivants sont à prendre en compte :

- Dans un environnement multiniveau en réseau, aucun stockage n'est effectué sur le réseau. Cependant, les grands parcs de serveurs sophistiqués peuvent employer un système d'équilibrage de charge (F5, par exemple) ; il peut donc y avoir un stockage de données de demandes HTTP qui affecte les valeurs d'horodatage. Ces périphériques dédiés étant personnalisables pour une vitesse améliorée, cet inconvénient passe presque inaperçu.
- Dans l'environnement, des périphériques de mise en cache de contenu peuvent déformer les valeurs temporelles. Lorsque le contenu est mis en cache, les valeurs temporelles sont réduites.
- Pour les pages plus volumineuses que la moyenne, il est plus efficace de compresser les données pour un transfert plus rapide.
- Si l'option de signal de présence HTTP/1.1 est activée, elle peut avoir des répercussions sur le taux de création des demandes HTTP.
- Les paramètres de distribution de l'application peuvent affecter la mesure des performances. La mise en mémoire tampon est-elle activée ? Par exemple, l'application commence-t-elle à transmettre lorsque le premier octet est prêt ou attend-elle plutôt que la page entière soit prête pour commencer ?
- Le regroupement en blocs affecte les valeurs temporelles. La réponse peut être renvoyée en un bloc ou encore en plusieurs blocs sur demande, comme par exemple un fichier PDF dont on ne sélectionne qu'une partie à l'aide du processus byte serving.
- Les paramètres du navigateur côté client peuvent affecter les valeurs temporelles et les performances. Si la mise en cache est activée, par exemple, les durées des transferts de pages ayant du contenu mis en cache sont réduites. La taille du cache est un facteur.

Horodatages dans les hits ReqCancelled

Lorsqu'une demande est annulée soit par le visiteur, soit par le serveur, les horodatages peuvent ne pas être insérés normalement selon l'heure à laquelle l'annulation a eu lieu. Tealeaf insère des horodatages en fonction du tableau ci-dessous.

Tableau 22. Horodatages dans les hits ReqCancelled

Action Current au moment de l'annulation	Horodatage de demande	Horodatage de réponse
Demande soumise, réponse pas encore démarrée (taille de la réponse = 0)	horodatage de demande	Utilisez la valeur RequestEndTimeEx
Demande soumise, réponse pas encore démarrée (Taille de la réponse > 0)	horodatage de demande	horodatage de réponse

Une réponse peut ne pas démarrer pour les raisons suivantes :

1. Annulation du visiteur
2. Annulation du serveur
3. Anomalie réseau
4. Le serveur a mis trop de temps à envoyer la réponse et le délai d'attente des paquets de la PCA a été dépassé
5. La PCA n'a pas pu faire correspondre la demande à la réponse

Remarque : Lors de la création de rapports à l'aide de l'événement `Req Cancelled Count`, vous pouvez regrouper les comptes de toutes les occurrences dans un tableau en précisant le type de données pour que l'événement devienne `[Sum]` à la place de `[Count]`. Reportez-vous au chapitre sur le générateur de rapport Tealeaf dans le document *IBM Tealeaf Reporting Guide*.

Hits sans horodatage

Si un hit est reçu avec des informations inexactes ou mal formatées sur l'horodatage, alors la PCA ne génère pas les horodatages associés.

Quand le hit est transmis au serveur de traitement pour évaluation, le serveur applique une valeur d'horodatage de `01/01/1970` au hit. Le hit est ensuite écrit dans un fichier de session avec le même horodatage.

Toutes les heures, le serveur de traitement supprime les plus anciens fichiers d'archive de la session en fonction de la limite de conservation des fichiers (en jours) définie dans le serveur de traitement. Les hits sont donc effacés automatiquement toutes les heures.

- La durée de conservation (en jours) des données par le serveur de traitement est définie dans l'onglet Services du canister du panneau de configuration du canister dans le système de gestion de Tealeaf. Voir section "Configuration du canister CX" dans le manuel de configuration d'*IBM Tealeaf CX*.

En plus des horodatages déformés ou manquants, les types de hits ci-dessous ne peuvent pas être horodatés :

1. Les hits de statistiques système de Tealeaf soumis par plusieurs des composants Tealeaf et qui ont pour rôle de rendre compte de l'état des composants ne peuvent pas être exclus du flux de capture du canister par l'agent de session du routeur de session.
   - Pour plus d'informations sur ces hits, voir section "Statistiques système" dans le manuel *IBM Tealeaf cxImpact - Guide d'administration*.
   - Voir section "Agent de session du routeur de session" dans le manuel de configuration d'*IBM Tealeaf CX*.
2. Si la base de données de recherche d'IBM Tealeaf cxReveal est déployée, les données insérées dans la base de données peuvent faire référence à ces hits. Lorsqu'une recherche IBM Tealeaf cxReveal est exécutée, les hits peuvent déjà avoir été purgés. Alors que la base de données indique l'existence des hits, ceux-ci n'existent pas dans les données du canister.
   - Pour plus d'informations sur cette anomalie, voir section "Traitement des incidents - cxReveal" dans le manuel de dépannage d'*IBM Tealeaf*.

     Remarque : La base de données de recherche d'IBM Tealeaf cxReveal doit être installée et configurée séparément. Voir section "Configuration de la recherche d'attributs de session" dans le manuel *IBM Tealeaf cxReveal - Guide d'administration*.

Notification des horodatages dans le portail et dans RTV

Le portail et RTV affichent trois valeurs générées par l'horodatage : la durée de création d'une page, la durée du déplacement réseau et la durée de l'aller-retour.

Durée de création d'une page

La durée de création d'une page correspond au temps qu'il faut à l'infrastructure Web (WS/AS/DB) pour traiter la réponse et pour commencer à la transmettre au navigateur client une fois qu'elle a reçu la demande. Cette valeur temporelle en microsecondes correspond à la durée qui sépare le moment où la PCA a vu le dernier paquet de la demande et celui où elle reçoit le premier paquet de la réponse. Elle est calculée puis insérée dans la demande en tant que `WS_Generation :`

```
WS_Generation = ResponseStartTimeEx - RequestEndTimeEx
```

Dans la demande ci-dessus présentée à titre d'exemple, la valeur temporelle `WS_Generation` correspond à `352928-347836 = 5092` microsecondes

Durée réseau

La durée réseau correspond à la différence entre le moment où le serveur Web commence à envoyer la réponse et celui où le visiteur fait part de la réception de ce paquet à la PCA. Elle est calculée puis insérée dans la demande en tant que `NT_Total :`

```
NT_Total = ResponseAckTimeEx - ResponseStartTimeEx
```

Dans la demande ci-dessus présentée à titre d'exemple, la valeur temporelle `NT_Total` correspond à `693390-352928 = 340462` microsecondes

Durée de l'aller-retour

La durée de l'aller-retour correspond à la différence entre le moment où la PCA reçoit le dernier paquet de la demande et celui où le visiteur lui fait part de la réception de la réponse dans son intégralité. Elle est calculée puis insérée dans la demande en tant que `RT_Total` :
`RT_Total = ResponseAckTimeEx - RequestEndTimeEx`

Dans la demande ci-dessus présentée à titre d'exemple, la valeur temporelle `RT_Total` correspond à :
`693390 - 347836 = 345554` microsecondes

Ce qui donne, si l'on examine les deux sections précédentes :

`RT_Total = WS_Generation + NT_Total`

Durée de rendu

Tealeaf UI Capture peut être déployé pour capturer les événements d'interface utilisateur dans le navigateur client et pour contrôler les valeurs côté client, comme par exemple la durée qu'il faut pour rendre la page dans le navigateur.

- Si UI Capture a été déployé, la durée de rendu est notifiée à Tealeaf en microsecondes. Pour plus d'informations sur UI Capture, voir section "FAQ UI Capture" dans la foire aux questions d'*IBM Tealeaf UI Capture for AJAX*.
- Pour plus d'informations sur UI Capture, voir section "Guide d'UI Capture for AJAX" dans le manuel d'*IBM Tealeaf UI Capture for AJAX*.
- Pour plus d'informations sur les données de performances distribuées via UI Capture, voir section "Analyse des performances" dans le manuel de notification d'*IBM Tealeaf*.

Test du traitement des performances par Tealeaf

Pour contrôler la vitesse à laquelle les hits sont traités par Tealeaf, vous pouvez utiliser le test suivant. Dans un système idéal, il s'écoule quelques secondes entre le moment où la PCA capture un hit et celui où le hit apparaît dans le canister à court terme.

Remarque : Si le canister à court terme envoie des hits au disque, le traitement est d'autant plus retardé et ce test ne permet pas d'indiquer avec fiabilité si les performances système sont fiables ou non. Voir "Etat du système" dans le manuel *IBM Tealeaf cxImpact - Guide d'administration*.

1. Connectez-vous au portail de Tealeaf.
2. Pour afficher les sessions actives en cours, sélectionnez **Active** > **Portail**. Triez les entrées affichées par heure.

   Remarque : Ces opérations peuvent prendre jusqu'à cinq secondes et introduire un décalage dans la mesure des performances.
3. Sur un ordinateur, ouvrez une horloge qui indique le décompte des secondes.
4. Enregistrez l'heure de début d'une nouvelle session.
   - Continuez à rafraîchir la page Sessions actives jusqu'à ce qu'une nouvelle session commence.
   - Démarrez une nouvelle session en parcourant l'application Web à l'aide d'une nouvelle fenêtre de navigation.

5. Dès qu'une nouvelle session apparaît, notez le nombre de secondes qui s'affiche.
6. Ouvrez la même session avec l'application Reali-Tea Viewer ou Browser-Based Replay.
   - Voir section "Guide d'utilisation de RealiTea Viewer (RTV)" dans le manuel d'utilisation d' *IBM Tealeaf RealiTea Viewer*.
   - Voir "CX Browser Based Replay" dans le manuel d'utilisation d'*IBM Tealeaf cxImpact*.
7. Dans le premier hit de la session, ouvrez la demande.
8. Dans la section `[timestamp]`, examinez la valeur correspondant à `ResponseTimeEx`.
9. La différence (en secondes) entre la valeur ci-dessus et le moment où la session démarre permet de fournir une estimation proche de la durée réelle nécessaire à Tealeaf pour traiter un nouveau hit dans le canister à court terme.

Génération de rapports

Les rapports basés sur les informations d'horodatage capturées et calculés par Tealeaf peuvent être configurés et passés en revue via le portail de Tealeaf.

- Pour plus d'informations sur le paramétrage des niveaux de temps, voir chapitre Mesure des performances.

Si vous déployez la bibliothèque d'IBM Tealeaf Capture d'interface utilisateur CX pour AJAX, des informations temporelles côté serveur supplémentaires seront disponibles dans les rapports basés sur le portail.

- Voir section "Analyse des performances" dans le manuel de notification d'*IBM Tealeaf*.

Références

- Pour plus d'informations sur la notification des niveaux de temps, voir section "Analyse des performances" dans le manuel de notification d'*IBM Tealeaf*.
- Pour plus d'informations sur la configuration des niveaux de temps, voir «Console Web de la PCA - Onglet Pipeline», à la page 101.

Chapitre 7. Configuration de Passive Capture sur Red Hat Enterprise Linux (RHEL)

Les sections suivantes contiennent des informations essentielles concernant la configuration de Passive Capture dans un environnement Red Hat Enterprise Linux :

- «Passive Capture sur RHEL - Configuration du DNS»
- «Passive Capture sur RHEL - Configuration des interfaces réseau», à la page 226
- «Passive Capture sur RHEL - Configuration du NTP», à la page 229
- «Passive Capture sur RHEL - Configuration de l'accès au port série», à la page 230

Passive Capture sur RHEL - Configuration du DNS

Cette section fournit une description succincte des fichiers de configuration pour le service de noms de domaine (DNS) qui est utilisé pour assurer la conversion entre les noms d'hôte et les adresses IP. Le fichier `/etc/nsswitch.conf` contrôle l'utilisation des fichiers de la base de données du système et des services annuaires. Lorsque le DNS est activé par le fichier `nsswitch.conf`, le fichier `/etc/resolv.conf` contrôle la manière dont les recherches sont effectuées. Une fois enregistrées, les modifications effectuées sur ces fichiers système prennent effet.

Vous pouvez aussi utiliser l'utilitaire graphique redhat-config-network afin de configurer le DNS. Celui-ci n'est disponible que si le pack redhat-config-network est installé. Ce pack et les commandes qu'il propose ne sont pas disponibles avec une installation minimale de RHEL.

/etc/nsswitch.conf

Les sections suivantes décrivent comment activer et désactiver le DNS.

Désactivation du DNS

Pour désactiver les recherches DNS :

1. Modifiez le fichier `/etc/nsswitch.conf`.
2. Placez un signe dièse (#) au début de la ligne `hosts: files dns`.
3. Après modification, cette ligne doit contenir le code suivant :

```
#hosts: files dns
```

Activation du DNS

Pour activer les recherches DNS :

1. Modifiez le fichier `/etc/nsswitch.conf`.
2. Retirez tout signe dièse (#) au début de la ligne `hosts: files dns`. Après modification, cette ligne ressemble à :

```
hosts: files dns
```


/etc/resolv.conf

Pour indiquer le domaine et les serveurs DNS :

1. Modifiez le fichier `/etc/resolv.conf`.
2. Si le DHCP est activé pour une interface réseau, le fichier `/etc/resolv.conf` est créé automatiquement par le client DHCP avec les serveurs DNS indiqués par le serveur DHCP.
   - Normalement, vous ne modifiez le fichier `/etc/resolv.conf` que lorsque vous utilisez des adresses IP fixes (statiques).
3. Le fichier `/etc/resolv.conf` doit spécifier le suffixe du nom de domaine à utiliser lorsqu'un nom d'hôte n'est pas complet.
4. Vous devez aussi indiquer le nom d'au moins un serveur DNS à utiliser pour la résolution de nom d'hôte et d'adresse IP. Voici un exemple de fichier `/etc/resolv.conf` pour les machines du domaine Tealeaf.com avec deux serveurs DNS :

```
search machines.tealeaf.com
nameserver 172.16.0.5
nameserver 172.16.0.6
```

Passive Capture sur RHEL - Configuration des interfaces réseau

Les fichiers de configuration du réseau dans le répertoire `/etc/sysconfig` sont lus et traités pendant l'initialisation du système. Pour effectuer des modifications, redémarrez la machine à l'aide de la commande `shutdown -r now`.

- Au lieu de redémarrer la machine, vous pouvez aussi la paramétrer en mode utilisateur unique à l'aide de la commande `shutdown now`. A l'invite de commande, saisissez la commande `exit` afin de quitter le mode utilisateur unique et revenir au mode multi-utilisateur, qui active les interconnexions réseau et permet le démarrage des interfaces réseau.

Exemple DHCP

Cet exemple permet de configurer une machine nommée capture.my.domain qui récupère ses informations réseau à l'aide de DHCP sur l'interface eth0.

Afin d'assurer un mappage nom d'hôte/adresse IP pour la machine, le fichier `/etc/hosts` contient la ligne suivante :

```
127.0.0.1 capture.my.domain capture localhost.localdomain localhost
```

Le fichier `/etc/sysconfig/network` contient la ligne suivante :

```
HOSTNAME=capture.my.domain
```

Le fichier `/etc/sysconfig/network-scripts/ifcfg-eth0` ne contient que les lignes suivantes :

```
BOOTPROTO=dhcp
DEVICE=eth0
ONBOOT=yes
```

Exemple ETHTOOL_OPTS

Toutes les interfaces réseau utilisées avec Passive Capture doivent être configurées pour un mode duplex intégral. Le mode duplex intégral assure une utilisation maximale des interfaces réseau pour la capture de paquets et la distribution de hits Tealeaf au service de transport Tealeaf.

Vous pouvez ajouter une variable intitulée ETHTOOL_OPTS au fichier ifcfg pour que l'interface réseau force le mode duplex. Vous devez généralement le faire lorsque l'appareil s'auto-négocie en mode semi-duplex. L'exemple de ligne suivant paramètre la variable ETHTOOL_OPTS afin de forcer l'utilisation du mode duplex intégral à 1 gigaoctet pour l'interface réseau.

```
ETHTOOL_OPTS="autoneg off duplex full speed 1000"
```

Vous devez préciser le mode duplex et la vitesse ensemble et dans l'ordre indiqué. L'auto-négociation doit être désactivée au préalable pour pouvoir ensuite paramétrer le mode duplex et la vitesse. Le mode duplex et la vitesse doivent être paramétrés ensemble afin d'empêcher le pilote périphérique de l'interface réseau de réinitialiser le mode duplex ou la vitesse une fois les changements effectués.

Avec la variable ETHTOOL_OPTS définie dans le fichier ifcfg pour une interface réseau, la commande ifup exécute l'utilitaire ethtool et lui transmet les options définies par la variable. Par exemple, si vous avez modifié ifcfg-eth0 comme indiqué dans l'exemple précédent, alors ifup exécute la commande :

```
ethtool -s eth0 ${ETHTOOL_OPTS}
```

La commande va renvoyer la sortie suivante :

```
ethtool -s eth0 autoneg off duplex full speed 1000
```

Les modifications effectuées sur le fichier ifcfg pour une interface réseau ne prennent effet que lorsque le script ifup s'exécute, ce qui correspond au moment où la machine démarre. Vous pouvez exécuter la commande ethtool manuellement pour que celle-ci prenne effet immédiatement. Par exemple :

```
ethtool -s eth0 autoneg off duplex full speed 1000
```

Exemple d'interface d'écoute

Cet exemple illustre la configuration de l'interface réseau eth2 pour la capture de paquets à partir d'un commutateur ou d'un TAP réseau.

Si la capture se fait à partir d'un commutateur, vous n'avez besoin que d'une interface réseau car il reçoit les données via un trafic bidirectionnel. Un TAP réseau envoie généralement des données via un trafic unidirectionnel (entrant et sortant) à l'aide de deux câbles réseau. C'est pourquoi, pour un TAP réseau, vous devez configurer deux interfaces réseau, une pour chaque câble. Dans les deux cas de figure, vous configurez l'interface réseau de la même manière. Une interface d'écoute n'a pas besoin d'une adresse IP car elle reçoit uniquement des paquets à partir d'un commutateur ou d'un TAP réseau. Elle n'envoie jamais de paquets sur le réseau câblé.

Le fichier /etc/sysconfig/network-scripts/ifcfg-eth2 ne contient que les lignes suivantes :

```
DEVICE=eth2
ONBOOT=yes
```

Exemple d'adresse IP statique

Cet exemple illustre la configuration d'une machine nommée `capture.my.domain` avec les informations réseau suivantes.

Paramètre
: **Valeur**

DNS
: `my.domain`

Nom d'hôte
: `capture`

Adresse IP
: `172.16.1.100`

Masque de réseau
: `255.255.255.0`

Passerelle
: `172.16.1.1`

Le fichier `/etc/hosts` contient les lignes suivantes :

```
127.0.0.1 localhost.localdomain localhost
172.16.1.100 capture.my.domain capture
```

Le fichier `/etc/sysconfig/network` contient la ligne suivante :

```
HOSTNAME=capture.my.domain
```

Le fichier `/etc/sysconfig/network-scripts/ifcfg-eth0` ne contient que les lignes suivantes :

```
BOOTPROTO=static
IPADDR=172.16.1.100
NETMASK=255.255.255.0
GATEWAY=172.16.1.1
DEVICE=eth0
ONBOOT=yes
```

Lecture complémentaire

Pour plus d'informations, consulter
Le guide Red Hat Enterprise Linux : répertoire sysconfig :
http://www.redhat.com/docs/manuals/enterprise/RHEL-3-Manual/ref-guide/ch-sysconfig.html

Le guide Red Hat Enterprise Linux : interfaces réseau :
http://www.redhat.com/docs/manuals/enterprise/RHEL-3-Manual/ref-guide/ch-networkscripts.html

Passive Capture sur RHEL - Configuration du NTP

Vous pouvez découvrir comment configurer un démon NTP afin de synchroniser l'heure de la machine avec au moins un serveur NTP. Tout d'abord, installez le pack NTP, celui-ci n'étant pas inclus dans une installation minimale. Après avoir installé le pack NTP, sélectionnez les serveurs NTP, créez des fichiers de configuration puis activez et démarrez le service.

Installation du pack NTP

Si ce n'est pas déjà fait, installez le pack NTP à partir de votre distribution Linux.

Sélection des serveurs NTP

Pour synchroniser l'heure sur votre poste de travail, le démon NTP qui s'y trouve contacte un ou plusieurs des serveurs NTP spécifiés dans le fichier de configuration `/etc/ntp.conf`. Si aucun serveur NTP n'est disponible sur le réseau local, procédez comme suit :

- Sélectionnez un serveur NTP public (accédez aux http://www.ntp.org/ **Listes des serveurs de temps publics** et cliquez sur un serveur). Si vous sélectionnez un serveur NTP public, lisez les règles d'engagement (sur la page d'accueil du site NTP, cliquez sur **Règles d'engagement**).
- Utilisez le pool de serveurs de temps NTP (accédez à http://www.pool.ntp.org/ **Comment utiliser pool.ntp.org ?** et cliquez sur le pool).

Connectez-vous en tant qu'utilisateur `racine` sur le poste de travail et vérifiez que la machine peut se connecter avec les serveurs NTP sélectionnés. Utilisez la commande `ntpdate` avec l'option de requête `-q`. Par exemple, pour interroger un serveur NTP avec l'adresse IP `1.2.3.4`, utilisez la commande suivante :

```
ntpdate -q 1.2.3.4
```

La sortie doit ressembler à l'exemple suivant qui affiche le serveur contacté et la différence d'heure entre le poste de travail local et le serveur.

```
server 1.2.3.4, stratum 2, offset 150.695779, delay 0.03366
17 Nov 10:27:09 ntpdate[21597]: step time server 1.2.3.4 offset 150.695779 sec
```

Si la requête échoue, la sortie qui est susceptible d'apparaître est la suivante :

```
server 1.2.3.4, stratum 0, offset 0.000000, delay 0.00000
17 Nov 10:29:04 ntpdate[21599]: no server suitable for synchronization found
```

Création des fichiers de configuration

Connectez-vous sur la machine en tant qu'utilisateur racine et procédez comme suit :

1. Créez le fichier /etc/ntp/step-tickers. Vous pouvez faire une sauvegarde de toutes les versions existantes du fichier. Le fichier contient les noms d'hôte ou les adresses IP des serveurs NTP à contacter pendant le démarrage afin d'effectuer une configuration initiale de l'heure. Si vous utilisez le pool de serveurs NTP, vous devez utiliser les noms d'hôte, ce qui requiert un DNS. Par exemple, si les deux serveurs NTP à utiliser sont 1.2.3.4 et 5.6.7.8, il vous faut alors utiliser les commandes suivantes pour créer le fichier :

```
echo 1.2.3.4 > /etc/ntp/step-tickers
echo 5.6.7.8 >> /etc/ntp/step-tickers
```

2. Créez le fichier /etc/ntp.conf avec les commandes suivantes. Vous pouvez faire une sauvegarde de toutes les versions existantes du fichier.

```
echo restrict default ignore > /etc/ntp.conf
echo restrict 127.0.0.1 >> /etc/ntp.conf
echo driftfile /var/lib/ntp/drift >> /etc/ntp.conf
```

3. Ajoutez des entrées à l'aide des mots clés restrict et server pour chaque serveur NTP. L'exemple suivant illustre l'ajout d'entrées pour les serveurs NTP hypothétiques 1.2.3.4 et 5.6.7.8. Les options mask, nomodify, notrap et noquery empêchent le serveur de modifier le service NTP sur la machine hôte de Passive Capture.

```
nullecho
restrict 1.2.3.4 mask 255.255.255.255 nomodify notrap noquery >> /etc/ntp.con
echo server 1.2.3.4 >> /etc/ntp.conf
echo restrict 5.6.7.8 mask 255.255.255.255 nomodify notrap noquery >> \
/etc/ntp.con
echo server 5.6.7.8 >> /etc/ntp.conf
```

Activation et démarrage du service

Connectez-vous sur la machine en tant qu'utilisateur racine et procédez comme suit :

1. Configurez le service afin de le lancer au démarrage à l'aide de la commande suivante :

```
chkconfig ntpd on
```

2. Lancez immédiatement le service à l'aide de la commande suivante :

```
service ntpd start
```

3. Vérifiez que le service est lancé et qu'il a contacté un serveur à l'aide de la commande suivante :

```
ntpq -np
```

4. Consultez les messages de journaux pour le démon NTP dans le fichier /var/log/messages.

Passive Capture sur RHEL - Configuration de l'accès au port série

Cette section donne des informations sur l'utilisation d'un port série sur le serveur de Passive Capture pour accéder à la console et au terminal.

Chapitre 8. Surveillance de Passive Capture

Cette section explique comment surveiller IBM Tealeaf Application de capture passive CX.

Liste de contrôle pour le diagnostic des anomalies de la PCA

La console Web de la PCA fournit des informations détaillées sur la marche à suivre pour diagnostiquer les anomalies avec IBM Tealeaf Application de capture passive CX. Vous pouvez utiliser la liste suivante afin de vérifier les opérations de la PCA à l'aide des onglets de sa console Web.

Liste de contrôle principale

1. **«Console Web de la PCA - Onglet Console», à la page 70** - Activation/désactivation de la capture passive.
   a. Vérifiez que la capture passive est activée.
2. **«Console Web de la PCA - Onglet Récapitulatif», à la page 60** - Contient des mesures et des informations d'état sur les processus, homologues et interfaces réseau individuels de la PCA. Les avertissements et messages d'erreur s'affichent ici. Vérifiez :
   a. Que tous les processus de capture sont prêts à s'exécuter.
   b. Que les homologues de distribution sont définis et connectés et qu'ils distribuent des hits
   c. Que les interfaces réseau sont prêtes.
      - Pour obtenir les statistiques sur une interface réseau, cliquez sur **(détails)**.
      - Pour plus de diagnostics, cliquez sur le lien **Utilitaires**.
      - Pour plus d'informations sur les messages qui s'affichent dans l'onglet récapitulatif, voir «Console Web de la PCA - Onglet Récapitulatif», à la page 60.
3. **«Console Web de la PCA - Onglet Interface», à la page 71** - Configuration de plusieurs instances de la PCA, des interfaces réseau, de la segmentation des données et des filtres de données. Cette section contient les paramètres de réglage des performances. Vérifiez :
   a. Que l'interface principale est prête et qu'elle écoute le trafic dans les deux directions.
   b. Que les directions de chaque interface sont correctement configurées. Voir «Console Web de la PCA - Onglet Interface», à la page 71.
   c. Que les numéros de port du trafic sont correctement paramétrés.
   d. Que les filtres du trafic ignoré ne filtrent pas des données requises.
   e. Si vous utilisez plusieurs instances de la PCA, vérifiez que toute configuration de la segmentation de données dirige le trafic vers l'instance appropriée.
   f. Que toutes les règles de filtrage définies comprennent ou excluent le trafic du port comme souhaité.
   g. Que les paramètres d'optimisation n'ont pas de répercussions sur les performances du système.

4. **«Console Web de la PCA - Onglet Distribution», à la page 92** - Définition et test des connexions afin de cibler les destinataires des données de la PCA. Activation et configuration de la distribution des statistiques de la PCA au pipeline de Windows. Vérifiez :
   a. Que les noms d'hôtes et les numéros de port cibles sont correctement définis
   b. Pour le diagnostic des anomalies, la distribution des hits de statistique de la PCA au pipeline de Windows permet un meilleur suivi des performances du système. Pour plus d'informations sur les hits de statistiques, voir «Statistiques par instance», à la page 137.

Liste de contrôle de configurations supplémentaires de la PCA

Pour les anomalies suivantes, suivez les instructions de la liste ci-dessous :

1. Anomalies relatives au protocole SSL - Si la PCA ne capture pas correctement le trafic HTTPS, reportez-vous à la configuration des clés SSL.
   - Vérifiez qu'il ne manque aucune clé privée.
   - Vérifiez sur le serveur Web que la clé SSL actuelle est exportée et fournie à la PCA.
   - Voir «Console Web de la PCA - Onglet Clés SSL», à la page 97.
   - La clé privée de serveur Web doit être exportée, convertie puis importée dans la PCA. Voir Chapitre 5, «Clés SSL», à la page 193.
2. Données sensibles - Si des données sensibles sont transmises via la PCA au pipeline et aux bases de données de Windows, vous pouvez paramétrer les règles de confidentialité afin de bloquer ou de masquer ces données dès qu'elles arrivent sur la PCA.
   - Vérifiez que les règles de confidentialité sont correctement paramétrées.
   - Passez en revue l'utilisation des expressions régulières dans les règles de confidentialité, celles-ci pouvant considérablement affecter la performance de la PCA.
   - Voir «Téléchargement de la configuration de confidentialité», à la page 118.
3. Anomalies relatives au basculement - Il est possible de configurer la PCA pour que celle-ci bascule de l'instance principale vers l'instance secondaire dès que nécessaire. Voir «Console Web de la PCA - Onglet Reprise», à la page 161.

Conseils supplémentaires pour le diagnostic des anomalies

Si la liste de contrôle ci-dessus ne vous a pas permis de repérer l'anomalie, vous pouvez passer en revue les éléments suivants pour vérifier les performances du serveur d'IBM Tealeaf Application de capture passive CX.

Dans certains cas, les anomalies qui apparaissent dans IBM Tealeaf Application de capture passive CX se produisent au niveau du système d'exploitation ou du réseau. Les conseils suivants sont des étapes de validation utiles à effectuer avant de contacter le service clients Tealeaf.

- Vérifiez l'espace disque sur le volume où la PCA est hébergée
- Vérifiez les processus du système d'exploitation
- Vérifiez l'historique récent des modifications effectuées sur la console Web de la PCA, celles-ci étant consignées dans le fichier suivant :
  ```
  /var/log/tealeaf/confxxx.log
  ```

- Vérifiez l'état des cartes d'interface réseau à l'aide d'outils externes tels que `ifconfig` et `ethtool`
- Vérifiez les connexions physiques entre le serveur, les cartes d'interface réseau et le réseau

Surveillance de Passive Capture via le statut de Tealeaf

Le rapport de statut Tealeaf, introduit dans la version 8.0, interroge chaque serveur Tealeaf actif configuré dans la page Gestion du portail pour obtenir des informations de statut et crée aussi un rapport récapitulatif dans le portail. Il fournit une vue d'ensemble de l'intégrité de votre système.

- Voir "Rapport de statut Tealeaf" dans le manuel *IBM Tealeaf cxImpact - Guide d'administration*.

Pour inclure la création de rapports sur la PCA dans le rapport de statut Tealeaf, activez l'application Portail à l'aide des instructions suivantes. Cette application communique avec le ou les serveur(s) qui hébergent la PCA.

1. Connectez-vous au portail en tant qu'administrateur Tealeaf.
2. Dans le menu Portail, sélectionnez **Tealeaf** > **Gestion du portail**.
3. Dans la page Gestion du portail, cliquez sur le lien **Gérer les serveurs** .
4. Passez en revue la liste des serveurs. Vérifiez que la liste contient une référence pour chaque serveur de la PCA dont vous voulez recevoir les informations de statut Tealeaf.
5. Si l'un des serveurs ne se trouve pas dans la liste, créez-lui une entrée :
   a. Cliquez sur **Nouveau**. Dans le menu déroulant, sélectionnez **Serveur applicatif de Capture**.
   b. En bas de la page, indiquez les propriétés permettant à l'application Portail de se connecter au serveur de la PCA.
   c. Vérifiez que la case Actif est cochée.
   d. Pour enregistrer l'entrée, cliquez sur **Enregistrer**.
   e. L'entrée doit s'afficher dans la liste des serveurs.
   f. Sélectionnez l'entrée. En haut de la liste des serveurs, cliquez sur l'outil **Ping** pour tester la connexion entre l'application Portail et le serveur.
      - Voir "Serveurs de gestion de Tealeaf" dans le manuel *IBM Tealeaf cxImpact - Guide d'administration*.
6. Répétez les étapes précédentes pour créer des entrées pour les autres serveurs de la PCA de l'environnement.
7. Lorsque vous avez fini de créer les entrées pour tous les serveurs de la PCA, générez un rapport de statut Tealeaf :
   a. Dans la page Gestion du portail, cliquez sur le lien **Journaux** dans le panneau de navigation qui se trouve sur la gauche.
   b. Cliquez sur le lien Voir le statut de Tealeaf.
   c. Le rapport de statut Tealeaf s'affiche.
   d. Recherchez la `PCA` dans le rapport.
      - Voir "Rapport de statut Tealeaf" dans le manuel *IBM Tealeaf cxImpact - Guide d'administration*.

Consignation pour l'application Passive Capture

IBM Tealeaf Application de capture passive CX utilise les journaux suivants.

Remarque : A partir de Red Hat 6, le mécanisme de connexion du système d'exploitation passe à RSYSLOG. Les versions d'IBM Tealeaf Application de capture passive CX qui ne sont pas compatibles avec RHEL 6 ne prennent pas en compte cette modification et ne mettent pas à jour les bons fichiers de configuration du système. Par conséquent, certains journaux de la PCA, comme par exemple `capture.log`, sont vides. N'installez pas une build de la PCA dans une version du système d'exploitation qui ne la prend pas en charge.

Journaux de la PCA

Stockage

`/var/log/tealeaf/`

Nom des fichiers journaux
Description

`capture.log`
Journal des messages principal de la PCA, comprenant les messages d'erreur et de démarrage

- L'évolution de ce journal est régulièrement enregistrée en fonction de sa taille.
- `syslog` est utilisé pour générer des messages. Les autres journaux utilisent des méthodes natives pour générer des messages.

`conf_changelog.log`
Journal des modifications dans la configuration de la PCA. Modifications apportées au fichier de configuration `ctc-conf.xml`.

`statistics_YYYYMMDD.log`
Instantané minute par minute des statistiques de la PCA

- L'évolution de ce journal est enregistrée quotidiennement.

`maintenance_YYYYMMDD.log`
Messages concernant la surveillance de l'intégrité de la PCA et la synchronisation horaire

- L'évolution de ce journal est enregistrée quotidiennement.

`privacy_changelog.log`
Modifie la configuration des paramètres de connexion et de confidentialité qui s'appliquent via la PCA.

Journaux du serveur Apache

Le serveur Apache sert la console Web de la PCA.

Nom du fichier journal
Description

`access_log`
Messages concernant les adresses URL des demandes non SSL d'Apache

`error_log`
Messages d'erreur durant l'exploitation d'Apache

`ssl_engine_log`
Messages concernant l'exploitation SSL d'Apache

`ssl_request_log`
Adresses URL des demandes SSL d'Apache

Chapitre 9. Configuration matérielle et installation du système d'exploitation

Ce chapitre décrit l'installation des configurations matérielles requises avec une installation minimale de Red Hat Enterprise Linux pour le logiciel Tealeaf Passive Capture.

IBM Tealeaf Application de capture passive CX (PCA) est considéré comme un logiciel réseau, tel qu'un commutateur réseau, qui peut être installé sur une plateforme prise en charge par Linux. Ce logiciel a été créé pour s'exécuter dans un environnement consacré à la capture et au traitement de volumes importants de paquets réseau. Ainsi, il s'agit du seul logiciel d'application qui doit disposer d'un serveur Linux. Il n'est pas fait pour être partagé avec d'autres applications générales.

Configuration matérielle

Voici la configuration matérielle recommandée :

- Bi-processeurs : processeur Intel Xeon à 2,8 GHz minimum
- 2 Go de RAM minimum
- Une unité de disque dur SCSI d'au moins 60 Go (non RAID)
- Des cartes réseau d'au moins 3 gigaoctets :
  - Deux cartes avec interface réseau intégrée d'au moins 3 Go (inclus dans la carte mère PowerEdge) et une carte réseau supplémentaire d'au moins 3 Go faisant partie de la liste des modèles pris en charge suivante :
    - Carte réseauIntel PRO/1000 MT Gigabit
    - Carte réseauIntel PRO/1000 MF Gigabit (pour les clients dotés de la fibre)
- Lecteur de CD-ROM
- Lecteur de disquette d'1,44 Mo

Pour les réseaux fibre

Lors du choix de la carte réseau Gigabit avec une interface fibre, veillez à bien sélectionner le type de connecteur approprié à l'environnement. Voici deux exemples de cartes réseau dont le type de connecteur est compatible avec le réseau fibre :

- Connecteur SC : carte réseau Intel PRO/1000 XF Gigabit
- Connecteur LC : carte réseau Intel PRO/1000 MF Gigabit

Etapes de la préinstallation

Avant d'entamer le processus d'installation, suivez les étapes ci-dessous :

1. Branchez un câble réseau opérationnel de votre réseau local sur le port réseau LAN. Ne branchez pas d'autre câble réseau dans les autres ports réseau.
2. Insérez le disque 1 du CD-ROM d'installation et de démarrage de Red Hat Enterprise Linux dans le lecteur de CD-ROM.
3. Mettez l'ordinateur sous tension.
4. Entrez la configuration BIOS et configurez l'horloge CMOS à l'heure moyenne de Greenwich (GMT).

5. Quittez le BIOS. L'ordinateur démarre et l'écran d'accueil d'installation de Red Hat Enterprise Linux s'affiche.
6. Appuyez sur la barre d'`espace` pour empêcher le démarrage automatique.
7. Reportez-vous à la section d'installation de Red Hat Enterprise Linux.

   Remarque : En général, le fuseau horaire de Passive Capture est configuré en fonction du fuseau horaire local. L'étape 4 permet la configuration et la modification du fuseau horaire de Passive Capture sans avoir à changer l'horloge CMOS.

Configuration générale

La section suivante contient des informations sur la configuration générale.

Désactivation des iptables

Sur le serveur de Linux qui héberge IBM Tealeaf Application de capture passive CX, désactivez les iptables.

Remarque : Si les iptables sont activées et qu'elles ne peuvent pas être désactivées, vous pouvez désactiver le pare-feu via Linux pour accéder à la console Web de la PCA. Pour plus d'informations, consultez la documentation fournie avec votre version de Linux.

Etapes :
Pour désactiver les iptables, exécutez les commandes suivantes dans l'ordre indiqué.

Remarque : Pour plus d'informations sur les iptables, consultez la documentation correspondant à votre version de Linux.

1. Commandes :
   ```
   service iptables save
   service iptables stop
   chkconfig iptables off
   ```
2. Redémarrez la PCA.

Hyper-Threading

Remarque : Si la PCA est hébergée sur un serveur qui prend en charge la fonction Hyper-Threading, ne la désactivez pas. Elle est activée sur la plupart des serveurs qui la prennent en charge et doit l'être pour IBM Tealeaf Application de capture passive CX. Voir Chapitre 2, «Installation», à la page 17.

Installation de Red Hat Enterprise Linux

Remarque : Lorsque vous effectuez des modifications dans la configuration de votre installation Linux, appliquez les modifications au fichier `runtime.conf` qui remplace le fichier `tealeaf.conf` par défaut. Ce dernier peut être utilisé pour annuler les modifications apportées aux paramètres par défaut si nécessaire et doit être configuré en lecture seule.

Désactivation de SELinux

Les fonctionnalités de Red Hat Linux permettant d'améliorer la sécurité ne sont pas compatibles avec IBM Tealeaf Application de capture passive CX. Plusieurs

paramètres système ne sont pas autorisés en mode SELinux et le système syslog n'est pas disponible, ce qui empêche le fichier `capture.log` de la PCA de fonctionner.

- Si SELinux est activé et que le script de tealeaf est utilisé pour démarrer la capture, un message d'avertissement s'affiche.
- Un message d'avertissement s'affiche aussi dans la console Web de la PCA lorsque SELinux est activé.

Avant d'installer IBM Tealeaf Application de capture passive CX, vous devez activer SELinux par le biais du système d'exploitation. Pour plus d'informations, voir la documentation de Linux.

RHEL5

Suivez les instructions de RHEL3, en notant les deux différences majeures pour l'installation de RHEL5 :

- Configuration du disque : pour étudier le disque et modifier les partitions, vous devez cocher la case intitulée **Vérifier** et modifier l'agencement des partitions à l'étape 8.
- Sélection des packs : l'écran de sélection des packs de RHEL5 est différent de celui de RHEL3 et 4. Il est divisé en six sections : environnement, applications, développement, serveurs, langues et système de base du bureau. Pour effectuer une installation minimale, ne laissez aucune case cochée à l'exception des cases **Outils d'administration** et **Articles de base** dans la section **Système de base**. Vous pouvez aussi installer les éditeurs dans la section **Applications**.

Sécurité de la console Web

La section suivante contient des informations sur la sécurité de la console Web.

Désactivation du serveur Web pour la console Web

Pour désactiver le serveur Web pour la console Web :

1. Exécutez la commande suivante :
   ```
   tealeaf disable httpd
   ```
2. Si la console Web est en cours d'exécution, arrêtez-la à l'aide de la commande suivante :
   ```
   tealeaf stop httpd
   ```
   - Si la commande précédente n'arrête pas le processus HTTPd, vérifiez qu'aucun utilisateur n'a la console Web ouverte dans une fenêtre de navigation.
   - Si l'exécution de la commande précédente échoue, vous pouvez utiliser la commande suivante pour arrêter tout processus HTTPd orphelin :
     a. Connectez-vous en tant qu'utilisateur racine.
     b. Exécutez la commande suivante :
        ```
        killall httpd
        ```
3. L'utilitaire du statut du portail a besoin du serveur Web pour récupérer les informations sur le statut. Si vous désactivez le serveur Web, l'utilitaire du statut du portail n'est plus en mesure de récupérer les informations sur le statut pour la PCA.

Désactivation de l'accès à la console Web à partir du port 8080

Pour désactiver l'accès à la console Web à partir du port 8080 :

1. Modifiez le fichier `/usr/local/ctccap/etc/runtime.conf`.
2. Recherchez la ligne suivante :
   ```
   httpd_port_enable=
   ```
3. Si la ligne n'existe pas, ajoutez-la.
4. Paramétrez la valeur "NO" après le signe égal. Par exemple :
   ```
   httpd_port_enable="NO"
   ```
5. Enregistrez le fichier.
6. Le fichier de configuration mis à jour prend effet au prochain démarrage du serveur Web.

Activation de l'accès à la console Web via une seule adresse IP

Pour autoriser l'accès à la console Web à partir d'une seule adresse IP :

1. Modifiez le fichier `/usr/local/ctccap/etc/runtime.conf`.
2. Recherchez la ligne suivante :
   ```
   httpd_console_allow_from=
   ```
3. Si la ligne n'existe pas, ajoutez-la.
4. Définissez la valeur située après le signe égal sur l'adresse IP à partir de laquelle vous accédez à la console Web. Par exemple :
   ```
   httpd_console_allow_from=1.2.3.4
   ```
5. Le fichier de configuration mis à jour prend effet au prochain démarrage du serveur Web.

Application de l'authentification pendant l'accès à la console Web

Si vous utilisez la procédure suivante pour restreindre l'accès à la console Web, vous devez utilisez le nom de fichier `index.php` lorsque vous accédez à la page par défaut de la console Web. Par exemple, après avoir effectué les étapes suivantes, l'URL ci-dessous ne s'affiche pas comme la page par défaut de la console Web pour l'adresse PCA 1.2.3.4.

```
http://1.2.3.4:8080/
```

Vous devez définir la page index.php comme suit :

```
http://1.2.3.4:8080/index.php
```

La restriction s'applique aussi à l'accès HTTPS suivant :

```
https://1.2.3.4:8443/index.php
```

Pour exiger un nom d'utilisateur/mot de passe lorsque vous accédez à la console Web :

Créez le fichier de base de données utilisateur du serveur Web à l'aide des commandes suivantes :

1. Modifiez le fichier `/usr/local/ctccap/etc/runtime.conf`.
2. Recherchez dans le fichier :

```
httpd_userauth_
```

3. Si la chaîne ne s'y trouve pas, ajoutez les paramètres suivants à la fin du fichier. Si ces entrées existent, définissez-les sur les valeurs suivantes :

   ```
   httpd_userauth_enable="YES"
   httpd_userauth_realm="PCAv2"
   httpd_userauth_require="valid-user"
   httpd_userauth_type="Basic"
   ```

   Remarque : Les valeurs pour `httpd_userauth_enable` doivent être en majuscules, comme dans l'exemple précédent (`YES`).
4. Pour ajouter un utilisateur ou modifier le mot de passe d'un utilisateur, utilisez l'une des commandes suivantes, en replaçant `johndoe` par le nom du nouvel utilisateur ou de l'utilisateur existant :
   - Lorsque la commande suivante s'exécute, il vous est demandé de saisir le mot de passe :

     Remarque : Tealeaf recommande l'utilisation de cette méthode pour créer des mots de passe. Si vous n'utilisez pas cette méthode, les mots de passe ne pourront pas dépasser huit caractères.

     ```
     /usr/local/ctccap/bin/htpasswd -m \
     /usr/local/ctccap/etc/tealeaf-web.users johndoe
     ```
   - Lorsque l'option `-b` est ajoutée, le mot de passe (`mypassword`) peut être spécifié dans la commande :

     ```
     /usr/local/ctccap/bin/htpasswd -mb \
     /usr/local/ctccap/etc/tealeaf-web.users johndoe mypassword
     ```
5. Les modifications mentionnées dans la commande précédente n'affectent pas l'emploi du serveur Web par l'utilitaire du statut du portail pour récupérer les informations sur l'état.
6. Le fichier de configuration mis à jour prend effet au prochain démarrage du serveur Web.

Application immédiate des modifications apportées à la configuration

Pour que les modifications effectuées sur le fichier de configuration `/usr/local/ctccap/etc/runtime.conf` prennent effet immédiatement :

Exécutez les commandes suivantes pour arrêter puis démarrer le serveur Web.

```
tealeaf stop httpd
tealeaf start httpd
```

Utilisateurs des systèmes d'exploitation

La PCA doit être installé via le compte utilisateur `racine`. Pendant le processus d'installation, l'utilisateur `ctccap` de la PCA est créé. Pendant l'exécution, l'utilisateur `ctccap` exécute les processus de la PCA indépendamment de l'utilisateur qui les a démarrés.

Remarque : N'utilisez pas l'utilisateur racine sudo pour l'installation. Même si celui-ci peut afficher que l'installation est terminée, plusieurs erreurs de capture indiquent que l'installation a échoué. Ces erreurs comprennent les erreurs de "redémarrage trop rapide", les tentatives de démarrage d'interface qui ont échoué, les anomalies se rapportant aux paramètres d'autorisations et bien plus. Assurez-vous d'être réellement connecté en tant qu'utilisateur racine.

Vous n'avez pas forcément à vous connecter au système en tant qu'utilisateur `racine`. Cependant, l'utilisateur `ctccap` doit avoir les autorisations nécessaires pour exécuter les commandes `tealeaf start` et `tealeaf stop`. Il est indispensable de les exécuter avec les autorisations `racines` limitées comme décrit précédemment.
En tant que trafic réseau capturant les exécutions d'applications fonctionnant sous un système d'exploitation de stock Linux, la PCA a besoin d'autorisations propres au système pour une capture passive des paquets réseau. Via le système d'exploitation, la PCA doit pouvoir placer les cartes d'interface du réseau du système dans un mode de capture de proximité. Cela permet à la PCA d'écouter passivement tout le trafic réseau présenté aux cartes réseau désignées. Il est indispensable d'exécuter le processus d'application spécifique avec les autorisations de l'utilisateur racine.

Pour réduire les anomalies relatives à la sécurité, seul un module d'application spécifique de la PCA a besoin de cette autorisation pour le trafic qu'il capture. Tous les autres modules d'application de la PCA ne s'exécutent pas sans autorisations de l'utilisateur racine.

- Le module de capture n'écoute qu'une copie du trafic réseau fourni. Il ne peut injecter aucun trafic quel qu'il soit entre votre serveur Web et le navigateur client.

Mises à niveau du système d'exploitation

Les sections suivantes contiennent des informations sur la mise à niveau des service packs et des systèmes d'exploitation .

Mise à niveau des service packs

Si vous mettez à niveau un service pack, plus aucune modification n'est requise une fois la mise à niveau terminée La PCA doit fonctionner correctement.

Mise en oeuvre de mises à niveau de versions majeures d'un système d'exploitation

Si vous effectuez la mise à niveau d'une version majeure d'un système d'exploitation, désinstallez d'abord la PCA avant d'exécuter la mise à niveau. Une fois la mise à niveau terminée, installez la nouvelle version de la PCA. Par exemple, si vous effectuez une mise à niveau de SLES9 vers SLES10, vous devez désinstaller PCA SLES9. Ensuite, effectuez une mise à niveau du système d'exploitation, vérifiez que celle-ci est réussie puis installez la version SLES10 de la PCA.

Chapitre 10. Maintenance de Passive Capture

Ce chapitre concerne l'utilitaire de maintenance de Passive Capture.

Présentation

L'utilitaire de maintenance effectue des tâches de routine pour Tealeaf Passive Capture. L'utilitaire effectue les tâches suivantes si celles-ci sont activées.

Diagnostic d'intégrité de la capture

L'utilitaire contrôle les processus de capture afin de déterminer s'ils fonctionnent correctement. Si l'utilitaire décide que ce n'est pas le cas, il effectue un redémarrage forcé. Le redémarrage forcé interrompt les processus de capture, efface les statistiques d'exécution collectées pour ensuite redémarrer les processus. Le diagnostic d'intégrité permet aux processus de capture de se remettre de situations qui altèrent leur efficacité et leurs performances. Si l'utilitaire de maintenance détermine que le processus de capture ne fonctionne pas correctement et qu'il doit être redémarré, il signale cette situation en écrivant un message au fichier journal de maintenance.

Redémarrage de la capture

En suivant un calendrier prédéfini, l'utilitaire interrompt les processus de capture et efface les statistiques d'exécution collectées. Il les redémarre ensuite chaque jour à une heure précise ou chaque semaine à une heure précise d'un jour précis. Le redémarrage forcé empêche les processus de capture de se trouver dans de mauvais état qui feraient échouer leur diagnostic d'intégrité.

Remarque : L'heure spécifiée (et le jour de la semaine, facultatif) doit correspondre à une heure où le processus de capture peut effectuer un redémarrage forcé sans avoir d'incidence sur la distribution des hits au service de transport Tealeaf. Les services comprennent une période de maintenance réseau de routine ou une période où les volumes de trafic des éléments à capturer sont faibles.

Emplacement des fichiers journaux

Pour IBM Tealeaf Application de capture passive CX, les fichiers journaux se situent dans le répertoire suivant :

```
/var/log/tealeaf
```

Une fois la PCA mise à niveau, l'emplacement des répertoires de fichiers journaux n'est jamais mis à jour. Si vous mettez votre PCA à niveau à partir d'une installation initiale antérieure à la build 3206, les fichiers journaux se trouvent alors à l'emplacement suivant :

```
/usr/local/ctccap/logs
```

Le répertoire de fichiers journaux est stocké dans le fichier suivant :

```
/usr/local/ctccap/etc/tealeaf.conf
```

Localisez l'entrée suivante :

```
logfiledir="/var/log/tealeaf"
```

Nettoyage des fichiers

Les fichiers journaux contrôlés par l'utilitaire se trouvent dans le répertoire /var/log/tealeaf et la date est comprise dans leur nom, par exemple statistics_20050602.log.

L'utilitaire contrôle l'âge et la taille des fichiers journaux spécifiés. Il les supprime aussi si leur durée de vie dépasse une période définie ou si leur taille est supérieure à celle définie.

Consignation des statistiques

L'utilitaire crée un fichier contenant plusieurs statistiques exécutées dans le temps. Ce fichier est destiné au débogage et au diagnostic de différents problèmes de capture et de distribution des hits.

Les fichiers journaux de statistiques sont créés dans le répertoire de journaux de la PCA qui correspond par défaut à l'emplacement suivant :

```
/var/log/tealeaf/
```

Les noms des fichiers journaux ont le format suivant : statistics_yyyymmdd.log.

- Les journaux ne sont jamais au format texte brut.
- Les anciens journaux se trouvent dans des fichiers compressés.

Conversion des fichiers journaux de statistiques au format de sortie

Pour une analyse plus poussée, vous pouvez, en cas de besoin, utiliser un script fourni par Tealeaf afin de convertir un fichier journal de statistiques PCA au format .csv ou .xml Le script se trouve à l'emplacement suivant :

```
/usr/local/ctccap/sbin/stat2csv
```

Remarque : Ce script suppose que la PCA est installée dans /usr/local/ctccap. Si la PCA est installée ailleurs, il faut modifier le shebang sur la première ligne du script afin qu'il mène à l'emplacement correct du binaire php : <pca install location>/bin/php.

Utilisation :

```
./stat2csv -t type -f infile -w outfile
```

où :

- infile - journal de statistiques en texte brut ou au format compressé.
- outfile - nom du fichier .csv ou .xml à sortir.
- type - type de fichier à sortir : CSV ou XML

Exemples :

```
./stat2csv -t csv -f statistics_20090406.log -w statistics_20090406.csv
./stat2csv -t xml -f statistics_20090406.log.gz -w statistics_20090406.xml
```

Synchronisation horaire

L'utilitaire synchronise la date et l'heure actuelles avec la date et l'heure actuelles d'un serveur d'IBM Tealeaf CX qui exécute le service de transport Tealeaf. Si celle-ci est activée, le fichier journal de maintenance contient alors le résultat de la tâche de synchronisation horaire effectuée.

Configuration manuelle

Pour configurer l'utilitaire de maintenance, vous devez modifier le fichier `/usr/local/ctccap/etc/runtime.conf` et y ajouter des lignes qui attribuent des valeurs aux variables.

- Les lignes commençant par un signe dièse ("#") correspondent à des commentaires et sont ignorées par l'utilitaire de maintenance.

L'attribution d'une valeur à une variable doit se faire sur une seule ligne dans le format suivant :

```
variable_name="value"
```

Remarque : Ne saisissez pas d'espace en début ou en fin de ligne, avant ou après le signe égal non plus. Ecrivez la valeur entre guillemets.

La liste suivante fournit des informations sur les variables de configuration, leurs valeurs par défaut (si celles-ci ne sont pas précisées dans le fichier `runtime.conf`) et leur signification.

- Plusieurs valeurs sont de type boléen et doivent être définies sur `YES` ou `NO`.

Diagnostic d'intégrité de la capture

```
capture_health_capture_packets_dropped_in_output_high_threshold="50000"
```

Si la statistique de capture `Packets dropped in output` est supérieure à cette valeur, le processus de capture ne fonctionne pas correctement. Cette valeur est élevée lorsque le processus de capture ne parvient pas à rassembler des hits aussi rapidement que si ceux-ci étaient capturés en dehors des interfaces réseau.

```
capture_health_enable="Yes"
```

- Active les diagnostics d'intégrité du processus de capture. Ce diagnostic est activé par défaut pour contrôler l'intégrité des processus de capture.

```
capture_health_reassd_pct_cpu_high_threshold="90"
```

- Si le processus de réassemblage de hits mobilise plus de 90% du processeur, la capture ne fonctionne pas correctement.

```
capture_health_reassd_virtual_size_high_threshold="1024000"
```

- Si le processus de rassemblement de hits mobilise plus d'un nombre déterminé de kilooctets (1 024 000 kilooctets correspondent environ à 1 gigaoctet), la capture ne fonctionne pas correctement.

```
capture_health_schedule_minutes="5"
```

- Nombre de minutes entre deux diagnostics d'intégrité.

Redémarrage de la capture

```
capture_restart_enable="NO"
```

- Effectue un redémarrage forcé des processus de capture à une heure donnée, soit chaque jour, soit chaque semaine à un jour donné. Ce diagnostic est désactivé par défaut car l'utilitaire ne trouve pas de période où le volume de trafic est assez faible ou sécurisé pour effectuer un redémarrage forcé. Pour l'activer, attribuez-lui la valeur `YES` et paramétrez l'heure du redémarrage des processus de capture dans la propriété suivante :

```
capture_restart_time_local="00:30"
```

- Redémarrez la capture à une heure locale donnée (à l'aide d'une horloge au format 24 heures). Si vous voulez redémarrer la capture à 23:30, utilisez la valeur "23:30". Ne mettez pas le zéro au début des heures inférieures à 10. Par exemple, pour indiquer 6:30, utilisez la valeur "6:30".

capture_restart_weekday_local (pas de valeur par défaut)

- Redémarrez la capture un jour de la semaine donné à une heure déterminée par la variable capture_restart_time_local.
- La valeur de cette variable doit être l'une des suivantes (tout en minuscule) : sunday, monday, tuesday, wednesday, thursday, friday ou saturday.
- Si vous spécifiez cette valeur, le redémarrage forcé intervient alors au jour et à l'heure spécifiés.
- Si vous ne configurez pas cette variable (et que vous la laissez la valeur par défaut), le redémarrage forcé intervient alors chaque jour à l'heure spécifiée.

Débogage

maintenance_debug_enable="NO"

- Active la consignation prolixe des paramètres et de l'exécution. Cette option existe afin d'aider à diagnostiquer le comportement de l'utilitaire de maintenance. Elle génère de nombreuses sorties dans le fichier maintenance.log et ne doit être utilisée qu'en cas de besoin.

Nettoyage des fichiers journaux

logfile_cleanup_enable="YES"

- Active le nettoyage des fichiers journaux.

logfile_cleanup_keepdays="14"

- Conserve les fichiers journaux pendant un nombre de jours donné. Les fichiers journaux ayant une durée de vie supérieure à ce nombre sont supprimés.
- Les noms des fichiers journaux contrôlés par l'utilitaire de maintenance contiennent une date au format <année><mois><jour>, par exemple 20050601 pour le 1er juin 2005.
- L'utilitaire se sert de la date extraite du nom de fichier et non de l'heure et de la date du fichier conservé par le système d'exploitation.

logfile_cleanup_keepsize_kb="5120"

- Conservez les fichiers journaux ayant une taille inférieure au nombre de kilooctets spécifié. La valeur par défaut conserve les fichiers journaux de taille inférieure à 5 mégaoctets environ.
- Les fichiers supérieurs à cette taille sont supprimés. Ce paramètre sert à empêcher les fichiers volumineux de s'accumuler sur la machine hôte de Passive Capture.

logfile_cleanup_schedule_minutes="30"

- Nombre de minutes entre deux diagnostics pour le nettoyage des fichiers journaux.

Consignation des statistiques

statistics_logging_enable="YES"

- Active la consignation des statistiques. S'il est activé, l'utilitaire de maintenance crée des fichiers CSV dans le répertoire /usr/local/ctccap/logs avec le nom statistics_YYYYMMDD.log, où YYYYMMDD correspond à l'année, au mois et au jour actuels, par exemple statistics_20050602.log.

statistics_logging_schedule_minutes="1"

- Nombre de minutes entre deux consignations des statistiques.

Synchronisation horaire

timesource_sync_enable="NO"

- Active la synchronisation horaire avec un serveur d'IBM Tealeaf CX qui exécute le service de transport Tealeaf.
- Les valeurs de configuration pour l'hôte et le port du service de transport Tealeaf se trouvent dans le fichier `/usr/local/ctccap/etc/ctc-conf.xml` et sont normalement attribuées via l'onglet Distribution de la console Web.
- Si les valeurs de configuration sont définies pour l'hôte et le port, l'utilitaire de maintenance active cette fonction par défaut. Sinon, l'utilitaire de maintenance désactive la synchronisation horaire.

`timesource_sync_schedule_minutes="15"`

- Nombre de minutes entre deux synchronisations horaires.

Annexe A. Annexes PCA

La section suivante contient les annexes concernant IBM Tealeaf Application de capture passive CX avec des informations de référence, des données de configuration supplémentaires ainsi que la foire aux questions.

Annexe B. Annexe - Cartes accélératrices prises en charge

Cette section fournit des informations sur les cartes accélératrices qui sont actuellement prises en charge par IBM Tealeaf Application de capture passive CX, y compris les instructions spécifiques concernant l'intégration.

Cartes accélératrices prises en charge

Tealeaf Passive Capture peut être utilisé avec les cartes accélératrices réseau suivantes :

Modèles de cartes accélératrices nCipher SSL :

- nCipher 6000 E
- Certains modèles de la série nFast/nForce 4000. Pour plus d'informations, contactez les services professionnels de Tealeaf.
- Voir Annexe C, «Système de gestion des clés nCipher SSL», à la page 251.

Annexe C. Système de gestion des clés nCipher SSL

Certaines installations Tealeaf utilisent une carte nCipher pour décharger le traitement du SSL à partir des processeurs principaux. La section suivante décrit comment paramétrer ce type de configuration.

Bien qu'il soit possible d'utiliser les cartes nCipher pour l'accélération SSL en déchargeant les opérations SSL sur la carte, leur objectif premier est de fournir une chambre forte sécurisée afin d'y conserver les clés SSL. Ce coffre est aussi connu sous le nom de module de sécurité matérielle (HSM) ou de système de gestion des clés nCipher.

Remarque : Les cartes nCipher n'offrent pas toutes une prise en charge du HSM.

Remarques relatives à nCipher

Le nombre d'instances qu'une carte nCipher peut gérer dépend de la série de la carte que vous possédez et du nombre de processeurs.

Remarque : nCipher peut modifier les valeurs standard de ses cartes accélératrices SSL. Pour travailler correctement avec Tealeaf PCA, les pilotes fournis avec la carte nCipher doivent fonctionner avec OpenSSL et fournir un accès transparent.

nCipher dispose de plusieurs modèles de cartes accélératrices SSL et de cartes de gestion des clés, chacune d'elles prenant en charge un nombre maximum différent de transactions SSL par seconde. Par exemple, une carte accélératrice nCipher SSL série 4000 peut gérer environ 4000 transactions maximum. La surcharge de la carte peut provoquer une réduction du pourcentage de sa capacité de traitement et ce nombre peut aussi diminuer en fonction du nombre d'instances de la PCA.

- Pour plus d'informations sur l'installation de plusieurs instances de la PCA, voir «Console Web de la PCA - Onglet Pipeline», à la page 101.

D'après l'exemple ci-dessus, la carte nCipher série 4000 a une capacité maximum d'environ 300-400 transactions par seconde pour une seule instance (SSL 1024 bits). Ce nombre peut varier en fonction du nombre d'instances de la PCA, il va généralement en diminuant.

Remarque : Evitez de fournir un trafic SSL supplémentaire à chaque instance de la PCA lorsque la capacité de traitement maximum de la carte accélératrice est atteinte.

Comatibilité d'IBM Tealeaf CX PCA et de nCipher

IBM Tealeaf CX PCA build 3611 et les builds ultérieures sont compatibles avec les utilitaires nCipher suivants :

- DES-CBC-SHA 56 SSL3, TLS1.0
- RC4-MD5 128 SSL3,TLS1.0,TLS1.1,TSL1.2
- RC4-SHA 128 SSL3, TLS1.0, TLS1.2
- AES128-SHA 128 SSL3, TLS1.0, DTLS1, TLS1.1, TLS1.2
- AES256-SHA 256 SSL3, TLS1.0, DTLS1, TLS1.1, TLS1.2
- DES-CBC3-SHA 192 SSL3, TLS1.0, DTLS1, TLS1.1, TLS1.2
- AES128-SHA256 128 TLS1.2
- AES256-SHA256 256 TLS1.2

Tealeaf PCA build 3610 et les builds antérieures sont compatibles avec les utilitaires nCipher suivants :

Remarque : PCA build 3328 ou ultérieure doit être déployé pour prendre en charge TLS 1.0.

- AES128-SHA 128 SSL3, TLS1.0, DTLS1
- AES256-SHA 256 SSL3, TLS1.0, DTLS1
- DES-CBC-SHA 56 SSL3, TLS1.0
- DES-CBC3-SHA 192 SSL3, TLS1.0, DTLS1
- RC4-MD5 128 SSL3, TLS1.0
- RC4-SHA 128 SSL3, TLS1.0

Installation de nCipher

Voir «Installation du HSM de nCipher pour la PCA», à la page 255.

Annexe D. Annexe - Intégration des clés SSL de Tealeaf avec HSM

Cette annexe décrit les méthodes d'intégration pour les fournisseurs HSM spécifiques. Un module de sécurité matérielle (HSM) fournit une protection à la fois logique et physique des données sensibles contre les utilisations non-autorisées et les ennemis potentiels.

Remarque : Ces méthodes d'intégration sont des approches généralisées intégrant Tealeaf avec les produits de chaque fournisseur. Afin de répondre aux besoins de votre environnement, la méthode décrite doit être personnalisée par un administrateur disposant de solides connaissances sur le produit HSM.

Dans un environnement avec HSM, le fichier de clés est stocké sur le HSM et conserve un contrôle d'accès renforcé qui prévient tout mouvement. Tealeaf créé des clés de référence afin d'accéder aux clés stockées sur le HSM. Les clés utilisées par l'exécution de Tealeaf obtiennent les mesures protectrices offertes par le HSM.

Méthodes d'intégration par le fabricant

- «Intégration avec le HSM de nCipher»
- «Installation du HSM de nCipher pour la PCA», à la page 255

Intégration avec le HSM de nCipher

La section suivante décrit une méthode générale pour intégrer Tealeaf avec des clés SSL stockées sur un module de sécurité matérielle (HSM) pour les produits nShield de nCipher.

- Cette méthode doit être personnalisée en fonction de votre solution HSM.
- Cette méthode s'applique à nShield et payShield de nCipher ainsi qu'aux ultra-modules payShield.

Hypothèses

Les hypothèses posées par cette méthode sont les suivantes :

- Vous avez installé le HSM dans votre environnement.
- Vous avez créé et configuré l'environnement sécurisé nCipher.
- Vous avez un accès de niveau administrateur à l'environnement sécurisé et vous maîtrisez son utilisation.

Exigences

Afin de fournir la meilleure prise en charge possible du HSM, celui-ci doit répondre aux exigences suivantes :

- Les pilotes fournis avec la carte doivent fonctionner avec OpenSSL.
- La carte doit être configurée afin de fournir un accès invisible au démarrage.
- Vérifiez que l'installation clé fonctionne au redémarrage du système.

Pour plus d'informations sur le respect de ces exigences, voir les interfaces d'application nCipher dans le manuel d'utilisation nShield/payShield fourni avec votre produit nCipher.

Si les conditions mentionnées ci-dessus sont respectées, Tealeaf peut accéder aux clés privées réelles, sans être vu, en créant un alias. Il peut aussi référencer les clés à l'aide des clés SSL qui lui sont fournies.

Configuration de PCA

Voir «Création d'un certificat autosigné», à la page 207.

Configuration et intégration du HSM

Afin d'intégrer Tealeaf avec le système de gestion des clés nShield de nCipher, appliquez ces instructions générales à votre environnement spécifique.

Remarque : Ces étapes ne sont qu'une référence générale et non pas une procédure d'installation pas à pas. Les étapes optionnelles suivantes supposent que vous êtes familier avec le logiciel de gestion des clés installé. Pour plus d'informations, reportez-vous au manuel nShield/payShield fourni avec votre produit nCipher.

Remarque : Afin de stocker les clés privées, le format PEM en texte brut peut être exigé pour les clés. L'utilitaire `generatekey` de nCipher crée les fichiers de clés PEM de référence équivalents. Passive Capture utilise ces fichiers de clés de référence pour la conversion au format chiffré PTL à l'aide de l'option de script `PEM2PTL` de Tealeaf. Pour plus d'informations, voir la partie Créer et importer des clés dans le manuel nShield/payShield.

Intégration

Pour intégrer :

1. Vérifiez que Linux et Passive Capture sont installés et que le serveur d'IBM Tealeaf Application de capture passive CX démarre correctement.
2. Vérifiez que la carte et le logiciel nCipher son correctement installés, ainsi que le lecteur de cartes à puce. Pour plus d'informations, voir la partie Tester l'installation dans le manuel d'utilisation nShield/payShield.
3. Installez le logiciel nCipher sur le serveur de la PCA.
4. Ajoutez le répertoire de bibliothèque CHIL de nCipher (`/opt/nfast/toolkits/hwcrhk`) au chemin de la bibliothèque de chargement du fichier `/etc/ld.so.conf`, si celui-ci n'y figure pas déjà.
5. Redémarrez le serveur de la PCA pour vérifier qu'il démarre correctement.
6. Exécutez la commande de liste des modules du noyau pour vérifier que le module de noyau (`lsmod`) de nCipher est chargé.
7. Sur le HSM, créez l'environnement sécurisé pour l'importation des clés.
8. Créez et/ou importez des fichiers de clés PEM dans le HSM.
   - Pour plus d'informations, voir la partie Créer et importer des clés dans le manuel d'utilisation nShield/payShield.
9. Vérifiez que les clés sont répertoriées dans le coffre de clés.
10. Sur le serveur de la PCA, exécutez l'utilitaire nCipher pour répertorier les clés dans l'environnement sécurisé de nCipher :

    ```
    /opt/nfast/bin/nfkminfo -l
    ```
11. Vérifiez que Passive Capture s'exécute et qu'il déchiffre le trafic SSL.

Désactivation du HSM

Afin de désactiver l'intégration du HSM au moment du démarrage de Passive Capture :

1. Créez un répertoire `DISABLED` dans `/etc/init.d`.
2. Déplacez les scripts nCipher du répertoire précédent au répertoire `DISABLED`.
3. Redémarrez Passive Capture.

Remarque : Cette procédure doit être effectuée avant de déplacer le matériel afin de permettre à Passive Capture de démarrer sans le module HSM (Hardware Security Module).

Instructions d'installation

Pour plus d'informations sur l'installation, voir «Installation du HSM de nCipher pour la PCA».

Installation du HSM de nCipher pour la PCA

Ces instructions d'installation s'appliquent aux séries de cartes de gestion des clés de nCipher compatibles avec IBM Tealeaf Application de capture passive CX.

Conditions préalables

Voici les instructions d'installation :

- HSM nShield 6000e
- Logiciel nCipher version 11.40
- Plateformes Linux validées, voir «Conditions préalables» pour une liste de plateformes prises en charge.

  Remarque : Si vous utilisez un système d'exploitation 64 bits, des bibliothèques 32 bits doivent être installées.

Bien que ces instructions ne soient pas approuvées, comme indiqué dans la section Prérequis, le logiciel nCipher et les plateformes Linux doivent aussi fonctionner pour les cartes suivantes :

- Cartes nForce/nFast/nShield plus antérieures à la série 4000

Conditions préalables supplémentaires

- Ces cartes peuvent être utilisées pour l'accélération SSL uniquement, mais les clés SSL sont toujours nécessaires pour que l'exécution se déroule correctement.
- Vous pouvez utiliser d'autres cartes nCipher qui ne prennent en charge que l'accélération SSL (pas de gestion des clés). Les pilotes doivent fonctionner avec OpenSSL de manière transparente (le pilote de la bibliothèque CHIL par exemple) et être configurés pour reconnaître OpenSSL automatiquement dès le démarrage. Vérifiez que l'installation fonctionne aussi au redémarrage du système.
- Si la carte nCipher doit être utilisée en tant que magasin de clés du HSM, il faut alors créer un environnement sécurisé nCipher. Voir «Création d'un environnement sécurisé nCipher pour la PCA», à la page 261.

Remarque : Pour réaliser les étapes optionnelles suivantes, vous devez connaître le logiciel de gestion des clés de nCipher. Ces étapes ne sont qu'une référence générale et non pas une procédure d'installation pas à pas. Si possible, faites appel

au centre d'aide de nCipher pour l'installation du logiciel car elle requiert généralement de compiler les pilotes du centre d'aide sur le système central.

Prérequis

Avant de commencer, vérifiez que les instructions suivantes ont été suivies ou effectuez-les.

1. La création du pilote de noyau nCipher nécessite la plateforme Linux nécessaire, vous devez donc l'effectuer sur un environnement de développement Linux installé sur la plateforme. Essayez de créer le pilote sur la machine de production attendue en premier lieu afin de déterminer si celle-ci permet la création d'un pilote à elle seule.

   Remarque : Pour la plateforme RHEL 5.6 64 bits, le pilote du noyau nCipher doit être créé pour des systèmes d'exploitation 64 bits. La PCA est une application 32 bits. La bibliothèque d'intercommunication de nCipher (`libnfhwcrhk.so`) doit donc être 32 bits elle aussi.
2. Une fois le pilote (`nfp.ko`) construit, vous pouvez appliquer le pilote `nfp.ko` créé et le logiciel de scripts de démarrage nCipher correspondant à l'ordinateur de production pour l'installation et le déploiement.
   - Pour plus d'informations, voir la documentation sur nCipher/Thales.
3. Ces instructions partent du principe qu'IBM Tealeaf Application de capture passive CX n'est pas encore installé.
   - Si la PCA est déjà installée, vous devez l'arrêter pendant que vous installez et intégrez le logiciel nCipher.
4. Voir «Importation des clés SSL dans le magasin de clés nCipher», à la page 263.

Etapes d'installation et de création de nCipher

Détails concernant la façon de créer et d'installer le pilote du noyau nCipher, de confirmer l'installation et de configurer les scripts de démarrage de nCipher pour un démarrage avant la PCA.

Création d'un pilote de noyau

1. Récupérez les éléments suivants du DVD de la version 11.40 de Linux (64 bits). Pour effectuer les commandes ci-dessous, le lecteur DVD doit être installé en tant que `/mnt/cdrom` :
   ```
   cd /
   tar xvf /mnt/cdrom/linux/libc6_3/amd64/nfast/hwsp/agg.tar
   tar xvf /mnt/cdrom/linux/libc6_3/amd64/nfast/ctls/agg.tar
   ```
2. Récupérez les fichiers suivants :
   a. Pour la PCA 32 bits, obtenez une version 32 bits de `libnfhwcrhk.so` :

      Remarque : `libnfhwcrhk.so` n'est fourni que comme fichier binaire et n'a pas été compilé localement. Ceci n'est pas une version spécifique à OpenSSL.
      1) Récupérez la version 32 bits du fichier suivant :
         ```
         tar xvf /mnt/cdrom/linux/libc6_3/nfast/hwcrhk/user.tar
         ```
      2) Lorsque le fichier `tar` précédent est extrait, il contient un fichier avec le chemin d'accès relatif à `libnfhwcrhk.so` :
         ```
         opt/nfast/toolkits/hwcrhk/libnfhwcrhk.so
         ```
      3) Copiez `libnfhwcrhk.so` dans le répertoire suivant :
         ```
         opt/nfast/toolkits/hwcrhk
         ```

b. Ces mêmes fichiers TAR stockés sur le DVD peuvent être extraits des fichiers ISO disponibles sur le site de téléchargement de nCipher. Récupérez les fichiers ISO suivants, contenant le logiciel nCipher nCSS :

```
nCSS_linux64_user_11_40.iso
nCSS_linux_user_11_40.iso
```

3. Une fois les commandes précédentes exécutées, la version non compressée du logiciel doit se trouver dans le répertoire suivant :

```
/opt/nfast
```

4. Pour créer le pilote du noyau nCipher (`nfp.ko`) :
   a. Pour les instructions, voir `nShield_Quick_Start_Guide.pdf` dans le répertoire de document du DVD de la version 11.40. Dans le chapitre 2, trouvez la partie Installation dans la section Linux, page 11.
   b. Le script de configuration recherche les en-têtes du noyau dans le répertoire défini par défaut (`/lib/modules/current_kernel_version/build/include`).
      1) S'ils se trouvent dans un autre répertoire, paramétrez la variable d'environnement `KERNEL_HEADERS` afin qu'ils soient dans le répertoire `$KERNAL_HEADERS/include/`. Pour plus d'informations, voir Paramétrage des variables d'environnement à la page 46 du document.
      2) En général, les en-têtes se trouvent dans `/usr/src/linux/include/`. Si les en-têtes pour votre noyau ne sont pas encore installés, installez-les à partir de votre disque de distribution ou contactez la personne qui vous a fourni les noyaux.
5. Commandes de création :

```
cd /opt/nfast/driver
./configure
make
```

6. Si l'utilisateur n'a pas été ajouté, exécutez la commande suivante :

```
useradd -r nfast
```

7. Validez le noyau en exécutant la commande suivante :

```
groups nfast
```

Installation du pilote du noyau nCipher

Remarque : Avant de commencer, vérifiez que la carte nCipher est installée sur le serveur de la PCA.

1. La commande suivante permet l'installation de `nfp driver.ko` et de ses scripts de démarrage.
   a. Commande :

   ```
   /opt/nfast/sbin/install
   ```

   b. Sélectionnez l'option `4`. Cette option peut être nécessaire pour l'ajout de `user:group`.
2. Ajoutez le chemin d'accès à la bibliothèque CHIL d'OpenSSL au fichier `ld.so.conf`, nécessaire pour la phase de redémarrage. Options :
   a. Option 1 :
      1) En passant par vi, ajoutez la ligne `/opt/nfast/toolkits/hwcrhk` au fichier suivant :

      ```
      vi /etc/ld.so.conf
      ```

      2) Exécutez la commande ldconfig -v afin de stocker une nouvelle entrée dans le fichier /etc/ld.so.cache
   b. Option 2 : exportez `LD_LIBRARY_PATH=/opt/nfast/toolkits/hwcrhk`

c. Option 3 : copiez la version 32 bits de /opt/nfast/toolkits/hwcrhk/libnfhwcrhk.so vers /usr/lib.

   Remarque : L'option 3 constitue l'approche recommandée mais elle ne peut pas être privilégiée en raison des différentes politiques d'administration système.

3. Si vous avez sélectionné l'option 1 ci-dessus, vous pouvez vérifier les entrées ld.so.cache existantes pour hwcrhk en exécutant le code suivant :

```
ldconfig -p |grep hwcrhk
```

Confirmation que le logiciel est installé

Selon l'option sélectionnée pour installer le logiciel, vérifiez qu'il se trouve dans l'un des répertoires suivants :

```
/opt/nfast/toolkits/hwcrhk/libnfhwcrhk.so
```

```
/usr/lib/libnfhwcrhk.so
```

Remarque : Pour réaliser ces étapes, l'installation du pilote du noyau doit être terminée. Voir «Installation du pilote du noyau nCipher», à la page 257.

1. Afin de vérifier que le pilote du noyau nfp est chargé, exécutez la commande suivante :

```
lsmod |grep nfp
```

2. La sortie attendue ressemble à :

```
nfp   42116    2
```

Correctif de démarrage

Si vous n'obtenez pas la sortie attendue, essayez d'arrêter puis de démarrer le pilote nCipher :

```
/opt/nfast/sbin/init.d-ncipher stop
/opt/nfast/sbin/init.d-ncipher start
```

Afin d'arrêter et de démarrer le serveur nCipher manuellement, exécutez la commande suivante qui est fournie avec la version 11.40 du logiciel :

```
/opt/nfast/sbin/init.d-ncipher start
/opt/nfast/sbin/init.d-ncipher stop
```

Deux nouveaux scripts de démarrage pour la version 11.40 du logiciel placés dans le répertoire /etc/init.d:

1. Démarrez les pilotes :

```
nc_drivers start
```

   où :

```
nc_drivers -> /opt/nfast/scripts/init.d/drivers
```

2. Démarrez le hardserver :

```
nc_hardserver start
```

   où :

```
nc_hardserver -> /opt/nfast/scripts/init.d/hardserver
```

Vérifiez que les scripts précédents fonctionnent pour une exploitation valide du pilote nCipher.

Remarque : Ceux-ci peuvent ne pas fonctionner au redémarrage. Les scripts de démarrage du lecteur de carte et du hardserver nCipher doivent être démarrés en premier lieu pour que la PCA les reconnaisse.

Installation du logiciel PCA

Si le logiciel PCA n'est pas encore installé, vous pouvez l'installer maintenant.

- Voir Chapitre 2, «Installation», à la page 17.

Configuration des scripts de démarrage de nCipher pour un démarrage avant la PCA

Les étapes suivantes permettent de configurer les scripts de démarrage de nCipher pour un démarrage ou un redémarrage avant l'exécution des scripts de démarrage de la PCA. Avant de pouvoir démarrer la PCA, la carte nCipher doit être initialisée.

Selon le système d'exploitation utilisé, procédez comme suit :

1. **«Configuration des scripts de démarrage pour RedHat»**
2. **«Configuration des scripts de démarrage pour SLES», à la page 260**

Configuration des scripts de démarrage pour RedHat

Pour les serveurs utilisant RedHat, procédez comme suit :

1. Configuration test :

1. Exécutez la commande de liste de démarrage des niveaux d'exécution :
   ```
   chkconfig --list |grep nc_
   ```
2. Si une liste est renvoyée, les scripts de démarrage nCipher définis par défaut ont été configurés correctement. Pour effectuer un test, redémarrez la PCA et confirmez qu'il s'agit du pilote de noyau nCipher. Voir «3. Contrôle de l'accès de la PCA au pilote du noyau nCipher», à la page 260.
3. Si aucune liste n'est renvoyée, les scripts de démarrage nCipher par défaut n'ont pas été configurés correctement. Voir «2. Configuration manuelle».

2. Configuration manuelle :

1. Les scripts de démarrage suivants doivent avoir les bons en-têtes de niveau d'exécution dans le fichier script pour pouvoir être reconnus :
   ```
   nc_drivers
   nc_hardserver
   ```
2. A l'aide d'un lien symbolique, les scripts de démarrage nCipher sont liés à :
   ```
   /opt/nfast/scripts/init.d/drivers
   /opt/nfast/scripts/init.d/hardserver
   ```
3. Modifiez les scripts de démarrage nCipher :
   a. Modifiez le fichier `/opt/nfast/scripts/init.d/drivers`. Ajoutez les lignes suivantes :
      ```
      # chkconfig: 2345 45 55
        # description: nCipher drivers
      ```
   b. Modifiez le fichier `/opt/nfast/scripts/init.d/hardserver`. Ajoutez les lignes suivantes :
      ```
      # chkconfig: 2345 50 50
      # description: nCipher hardserver
      ```
   c. Par exemple :

```
#!/bin/sh
# generated by inst-def.sh
# chkconfig: 2345 45 55
# description: nCipher drivers
```

4. Le système peut avoir besoin de quelques minutes pour ajouter automatiquement les scripts à la liste `chkconfig --list`. Si les scripts ne s'affichent pas, activez alors les niveaux d'exécution manuellement comme indiqué dans les instructions suivantes :
   a. Utilisez chkconfig pour activer le niveau d'exécution `2,3,4,5` pour `nc_drivers` et `nc_hardserver`.

      ```
      chkconfig --level 2345 nc_drivers on
      chkcofnig --level 2345 nc_hardserver on
      ```

5. Confirmez que la PCA peut accéder au pilote du noyau. Voir «3. Contrôle de l'accès de la PCA au pilote du noyau nCipher».

3. Contrôle de l'accès de la PCA au pilote du noyau nCipher :

1. Redémarrez la PCA.
2. Après le démarrage, exécutez la commande suivante :

   ```
   # lsmod |grep nfp
   ```

3. La sortie est la suivante. Le code `2` indique 'utilisé par' :

   ```
   nfp   42116    2
   ```

4. Pour confirmer que les scripts de démarrage de la PCA et nCipher ont les bonnes priorités
   de démarrage, les exemples suivants indiquent que nCipher démarre en premier, suivi par la PCA :

   ```
   /etc/rc.d/rc2.d/S45nc_drivers
   /etc/rc.d/rc2.d/S50nc_hardserver

   /etc/rc.d/rc2.d/S60tealeaf-pca
   /etc/rc.d/rc2.d/S55tealeaf-startup
   ```

5. Après avoir suivi les instructions ci-dessus, vous devez vous assurer que le pilote du noyau nCipher est bien visible par la PCA. Voir «Contrôle de l'utilisation des clés privées SSL», à la page 264.

Configuration des scripts de démarrage pour SLES

Remarque : Ces instructions s'appliquent aux versions 11.40 et ultérieures de nCipher, sauf indication contraire.

Vérifiez que nCipher se lance correctement avec la PCA. A partir de la version 11.40 de nCipher, deux scripts de démarrage (liens symboliques) sont fournis dans les répertoires suivants. Pour que nCipher se lance correctement, ces scripts doivent être exécutés dans l'ordre indiqué ci-dessous :

1. `/etc/init.d/nc_drivers`
2. `/etc/init.d/nc_hardserver`

   Remarque : Pour que nCipher soit reconnu correctement, ses scripts de démarrage doivent être exécutés avant ceux de Passive Capture.

1. Solution de contournement au démarrage :

Remarque : Le fait que la séquence de démarrage ne fonctionne pas correctement avec SUSE SLES peut créer des anomalies.

Etapes :
Pour SLES, la solution de contournement suggérée est la suivante.

1. Désactivez les niveaux d'exécution pour `nc_drivers` et `nc_hardserver` :
```
chkconfig -s nc_drivers off
chkcofnig -s nc_hardserver off
```
2. Réactivez-les avec les niveaux d'exécution `3` et `5` :
```
chkconfig -s nc_drivers on 3 5
chkcofnig -s nc_hardserver on 3 5
```
3. Par défaut, la priorité pour les scripts de chaque niveau d'exécution est définie à S01. Modifiez la priorité des niveaux d'exécution du démarrage de chacun de ces scripts dans les répertoires `rc3.d` et `rc5.d` à l'aide des commandes suivantes :
```
mv /etc/rc.d/rc3.d/S01nc_drivers /etc/rc.d/rc3.d/S09nc_drivers
mv /etc/rc.d/rc5.d/S01nc_hardserver /etc/rc.d/rc5.d/S10nc_hardserver
```

2. Vérification du pilote nCipher :

1. Après le démarrage, pour vérifier que le pilote nCipher est chargé correctement, utilisez la commande suivante :
```
lsmod |grep nfp
```
2. La sortie attendue doit ressembler à :
```
nfp   42116    2
(où '2' est attendu)
```

Après avoir suivi les instructions ci-dessus, vous devez vous assurer que le pilote du noyau nCipher est bien visible par la PCA. Voir «Contrôle de l'utilisation des clés privées SSL», à la page 264.

Création d'un environnement sécurisé nCipher pour la PCA

Remarque : Si la carte nCipher doit être utilisée comme un magasin de clés HSM, il faudra alors créer un environnement sécurisé nCipher. Les instructions suivantes s'appliquent à la création d'un environnement sécurisé nCipher avec quelques modifications spécifiques à IBM Tealeaf Application de capture passive CX. Ces instructions sont valables pour :

- nCipher nShield 4000
- nCipher nShield 6000e

Si votre environnement réseau nécessite un ensemble de règles différent ou des configurations supplémentaires, reportez-vous à `nShield_Quick_Start_Guide.pdf` pour des instructions plus détaillées.

1. Branchez le lecteur de carte à puce et insérez-y une carte. Une lumière verte sur le lecteur indique que la connexion est bonne.

   Remarque : Pour créer un magasin de clés d'environnement sécurisé, le lecteur de carte à puce doit être branché avec une carte permettant l'écriture du groupe de cartes à puce AES.
   a. L'importation de clés SSL ne requiert pas le branchement du lecteur de cartes pour la norme de sécurité FIPS140-2 de niveau 2 par défaut.
   b. Le lecteur de cartes doit être installé pour exécuter la PCA à l'aide du magasin de clés de l'environnement sécurisé pour ses clés SSL.
2. Créez un environnement sécurisé. Pour plus d'informations, voir `nShield_Quick_Start_Guide.pdf` page 13.
3. Connectez-vous à l'ordinateur hôte en tant qu'utilisateur du groupe nfast.

4. Mettez l'interrupteur du module qui se trouve sur le panneau arrière de nShield sur la position I correspondant au mode de préinitialisation.
5. Pour supprimer le module, exécutez la commande suivante :

   ```
   /opt/nfast/bin/nopclearfail ca
   ```

6. Exécutez la commande suivante :

   ```
   /opt/nfast/bin/new-world -m 1 -s 0 -Q 1/2 -k rijndael
   ```

7. La commande précédente permet de créer un environnement sécurisé FIPS conforme de niveau 2, où la reprise et le remplacement d'OCS sont activés, ainsi qu'un demi ACS. Le monde sécurisé est protégé par une clé AES.
   a. La commande précédente permet de créer deux cartes à puce ACS, mais une seule est nécessaire pour un accès sécurisé.
   b. Pendant le processus de création des cartes à puce, vous devez saisir une phrase de passe. Par exemple :

      ```
      ACS smartcard test passphrase:  testcard123
      ```

   c. Ce processus dure une à deux minutes par carte.
   d. Une fois l'environnement sécurisé créé, un message ressemblant au suivant doit s'afficher :

      ```
      Security World generated on module #1;
      hknso = 26b0b0fed1e2753c665b34af15523ebbb2a995a3
      ```

8. Placez l'interrupteur du module qui se trouve sur le panneau arrière de nShield sur la position O correspondant au mode opérationnel.

Validation de l'environnement sécurisé

Pour confirmer que l'environnement sécurisé a été correctement créé, procédez comme suit.

1. Exécutez la commande suivante :

   ```
   /opt/nfast/bin/nfkminfo
   ```

2. La sortie attendue doit être la suivante, `Usable` indiquant que la validation a été correctement effectuée :

   ```
   World
     generation  #
     state       0x17270000 Initialised Usable ...
     ...
   Module #1
     generation  #
     state      0x2 Usable
   ```

3. Pour plus d'informations sur l'ajout de clés SSL au magasin de clés de l'environnement sécurisé nCipher, étudiez les instructions permettant d'utiliser la commande suivante :

   ```
   /opt/nfast/bin/generatekey
   ```

   - Voir «Importation des clés SSL dans le magasin de clés nCipher», à la page 263.
4. La sortie de cette commande correspond à une clé de référence `.pem`. Cette clé doit être convertie au format `.ptl` utilisé par la PCA. Pour convertir le fichier de clés de référence en clé `.ptl`, utilisez la commande suivante :

   ```
   tealeaf pem2ptl <nCipherReference>.pem
   ```

5. Les clés `.ptl` de la PCA qui viennent d'être créées peuvent désormais être chargées dans la PCA et comprises par cette dernière :
   a. Pour une conversion manuelle : voir «Paramétrage des clés SSL chiffrées», à la page 193.
   b. Pour une conversion automatique : chargez les clés dans le répertoire par défaut :

```
/usr/local/ctccap/etc/capturekeys
```

Remarque : Vous devez créer ce répertoire et activer les permissions d'accès nécessaires. Voir «Paramétrage des clés SSL chiffrées», à la page 193.

6. Après avoir suivi l'une de ces méthodes, les clés `.ptl` sont chargées pour que la PCA puisse les utiliser.

Importation des clés SSL dans le magasin de clés nCipher

Pour stocker des clés SSL privées qui vont être utilisées par la PCA, celles-ci doivent être au format PEM en texte brut. L'utilitaire de nCipher, `generatekey`, crée les fichiers de clés PEM équivalents et ceux-ci peuvent ensuite être convertis pour que la PCA puisse les utiliser.

Voici une description de la procédure générale permettant d'importer des clés SSL dans le magasin de clés de
nCipher.

Pour installer le système de gestion des clés de nCipher :

1. Vérifiez que Linux est bien installé.
2. Installez la carte nCipher.
3. Installez le logiciel nCipher, qui permet la création des répertoires `/opt/nfast/...`, des scripts nfast et ainsi de suite.
4. Ajoutez le répertoire de bibliothèque CHIL de nCipher au chemin de la bibliothèque de chargement, `/opt/nfast/toolkits/hwcrhk`, ainsi qu'au fichier `/etc/ld.so.conf`, s'il ne s'y trouve pas déjà.
5. Vérifiez que le logiciel Passive Capture est installé.
6. Relancez le serveur d'IBM Tealeaf Application de capture passive CX pour vérifier qu'il démarre correctement.
7. Exécutez la commande de liste des modules du noyau pour vérifier que le module de noyau nfp lsmod de nCipher est bien chargé.
8. Créez l'environnement sécurisé nécessaire à l'importation des clés.
9. Importez les fichiers de clés RSA et PEM dans l'environnement sécurisé nCipher à l'aide de son utilitaire, `/opt/nfast/bin/generatekey`.
   Par exemple :
   ```
   /opt/nfast/bin/generatekey -i embed
   ```
   a. Cet exemple n'est valable que si les clés sont stockées sur le disque dans un format chiffré.
      1) Exécutez la commande suivante :
         ```
         [root@tstsys]# /opt/nfast/bin/generatekey -i embed
         ```
      2) S'affiche alors l'invite suivante :
         ```
         protect: Protected by? (token, softcard, module) [module] >
         ```
      3) Appuyez sur la touche `Entrée` pour accepter les valeurs par défaut. Ensuite, à l'invite :
         ```
         pemreadfile: PEM file containing RSA key? []
         ```
      4) Saisissez le fichier de clés privé : `tealeaf-web.pem`. Ensuite, à l'invite :
         ```
         embedsavefile: Filename to write key to? []
         ```
      5) Saisissez le nom du fichier de référence et l'emplacement d'écriture : `tealeaf-web_ref.pem`. Ensuite, à l'invite :
         ```
         plainname: Key name? []
         ```
      6) Saisissez l'alias de la clé : `tealeaf-web`.

7) Appuyez sur la touche `Entrée` pour les invites restantes afin d'accepter les valeurs par défaut.

10. Il se peut que vous deviez activer l'invite interactive pour les informations restantes.
11. Exécutez l'utilitaire de nCipher pour répertorier les clés dans l'environnement sécurisé :

```
/opt/nfast/bin/nfkminfo \-l
```

Contrôle de l'utilisation des clés privées SSL

A l'aide du journal de capture de la PCA, vous pouvez vérifier que celle-ci est capable de voir et d'utiliser la carte nCipher. Au démarrage, vous devez voir dans le fichier `capture.log` de la PCA le message suivant :

```
May 26 15:30:11 mammoth reassd[22722]: OpenSSL hw engine(1): CHIL hardware
engine support
```

Le journal doit aussi indiquer le nombre de clés :

```
Aug 20 16:53:37 mammoth reassd[10889]: Loaded 1 keys from Capture.CaptureKeys.
```

Une erreur survenue durant la tentative d'accès à la carte nCipher entraîne le message suivant :

```
hw engine(0)
```

Désactivation du lancement de nCipher lors du démarrage de Passive Capture

Remarque : Cette procédure doit être effectuée avant de retirer le matériel nCipher afin de permettre à Passive Capture de démarrer sans lui.

1. Créez un répertoire `DISABLED` dans `/etc/init.d`.
2. Si le script `nfast` est présent, déplacez-le du répertoire `/etc/init.d` vers le répertoire `DISABLED`.
3. Si vous utilisez la version 11.40 du logiciel ou une version ultérieure, déplacez les deux scripts `nc_drivers` et `nc_hardserver`, du répertoire `/etc/init.d` vers le répertoire `DISABLED`.
4. Dans `/usr/lib`, renommez le fichier `libnfhwcrhk.so` pour y ajouter l'extension `.disabled`

   ```
   mv libnfhwcrhk.so libnfhwcrhk.so.disabled
   ```

5. Redémarrez Passive Capture.

Annexe E. Annexe - Rubriques Passive Capture supplémentaires

Cette section contient des rubriques supplémentaires à propos d'IBM Tealeaf Application de capture passive CX sous forme de questions-réponses. Pour obtenir une réponse à l'une des questions suivantes, cliquez sur le lien.

Système d'exploitation

- «Passive Capture prend-il en charge la version 64 bits de Linux ?», à la page 266
- «Passive Capture prend-il en charge FreeBSD», à la page 266

Installation

- «Comment rendre l'installation et la configuration de la PCA automatiques ?», à la page 267
- «De quels packs le RPM tealeaf-pca a-t-il besoin ?», à la page 267
- «Quelles modifications le RPM tealeaf-pca effectue-t-il sur le serveur de la PCA ?», à la page 268
- «Comment définir le répertoire pour le lien symbolique de tealeaf ?», à la page 270
- «Comment désactiver la création d'un lien symbolique tealeaf ?», à la page 270
- «Comment effectuer l'installation dans un autre répertoire que celui défini par défaut ?», à la page 270
- «Quels répertoires et quels fichiers ne se situent pas dans le répertoire d'installation ?», à la page 271

Configuration du serveur Web

- «Comment retirer le système de chiffrement Diffie-Hellman de la liste des chiffrements SSL de serveur Web ?», à la page 273
- «Certains hits SSL n'apparaissent pas dans les sessions de navigation de Firefox», à la page 275

Configuration de la PCA

- «Comment définir d'autres fichiers de configuration ?», à la page 277

Console

- «Pourquoi la console Web de la PCA ignore-t-elle les modifications que j'ai enregistrées ?», à la page 279
- «Pourquoi est-il impossible d'interrompre les processus de la console Web ?», à la page 279

Journaux

- «Où se trouve le répertoire de journaux ctccap ?», à la page 280
- «Comment modifier le répertoire de fichiers journaux manuellement ?», à la page 280

Autre

- «Comment la PCA identifie-t-elle les pages ReqCanceled ?», à la page 283
- «Comment la PCA gère-t-elle la duplication des paquets TCP ?», à la page 282
- «Comment faire pour que la PCA efface automatiquement ses statistiques ?», à la page 281
- «Quel est le numéro de port par défaut correspondant au basculement ?», à la page 282
- «Comment la PCA gère-t-elle la capture des adresses IPv6 ?», à la page 289

Traitement des incidents

Pour plus d'informations concernant le traitement des incidents, voir "Traitement des incidents - Capture" dans le manuel de dépannage d'*IBM Tealeaf*.

Passive Capture prend-il en charge la version 64 bits de Linux ?

Question

Passive Capture prend-il en charge la version 64 bits de Linux ?

Réponse

Tealeaf ne fournit pas encore de version 64 bits d'IBM Tealeaf Application de capture passive CX pour les distributions 64 bits de Red Hat Enterprise Linux (RHEL) et de SUSE Linux Enterprise Server (SLES).

Cependant, vous pouvez installer la PCA sur un système d'exploitation 64 bits. Tealeaf ne fournit qu'un pack 32 bits qui dépend des bibliothèques 32 bits. Ces bibliothèques ne sont pas incluses dans les installations minimales des distributions 64 bits de RHEL, il faut donc les installer avant d'installer la PCA.

Remarque : Pour effectuer l'installation d'IBM Tealeaf Application de capture passive CX sur une version 64 bits de Linux, vous devez installer les versions 32 bits des packs dont votre système d'exploitation a besoin. Voir Chapitre 2, «Installation», à la page 17.

Passive Capture prend-il en charge FreeBSD

Question

Passive Capture prend-il en charge le système d'exploitation FreeBSD ?

Réponse

FreeBSD n'est plus pris en charge.

Remarque : Les clients qui utilisent la PCA sur un système d'exploitation non pris en charge ou sur une version non prise en charge d'un système d'exploitation qui l'est ne pourront pas obtenir d'aide concernant les problèmes liés au processus de capture.

Plusieurs versions majeures antérieures de Tealeaf prenaient en charge FreeBSD, un système d'exploitation similaire à UNIX. Tealeaf n'a pas été testé IBM Tealeaf Application de capture passive CX sur FreeBSD puisqu'il a commencé à prendre en charge Linux.

Le plus gros problème potentiel avec une version non prise en charge est l'établissement de liaison entre la PCA et les services de transport sur les serveurs Windows de Tealeaf.

Dans l'idéal, les clients qui utilisent actuellement des systèmes d'exploitation non pris en charge doivent changer pour l'une des versions prises en charge disponibles dans les liens «Références» ci-dessous.

Références

require-text

Configuration matérielle de la PCA et installation du système d'exploitation

- Chapitre 9, «Configuration matérielle et installation du système d'exploitation», à la page 235

Installation de la PCA

- Chapitre 2, «Installation», à la page 17

Comment rendre l'installation et la configuration de la PCA automatiques ?

Question

Comment faire pour rendre l'installation et la configuration de la PCA automatiques ?

Réponse

Remarque : Cette solution nécessite la version de `tpcinstaller.sh` du 05/07/2005, Révision 17, ou une version ultérieure.

Vous pouvez utiliser le script `tpcinstaller.sh` pour automatiser l'installation et la configuration du pack tealeaf-pca. Après l'installation, le script se trouve dans le sous-répertoire `bin`, mais vous pouvez aussi le demander auprès de Tealeaf.

Références

- Chapitre 2, «Installation», à la page 17

De quels packs le RPM tealeaf-pca a-t-il besoin ?

Question

De quels packs le RPM tealeaf-pca a-t-il besoin ?

Réponse

Utilisez la ligne de commande suivante pour que le RPM affiche la liste des packs dont le fichier de pack intitulé `abc.rpm` a besoin :

```
rpm -q --requires -p abc.rpm | fgrep -v rpmlib | sort -u | while read x; \
  do rpm -q --whatprovides "\${x}"; done | sort -u
```

Remarque :

- Exécutez la commande en tant qu'utilisateur racine.
- Remplacez le nom du fichier `abc.rpm` par le nom du fichier que vous voulez interroger.
- La commande utilise la syntaxe de l'interpréteur de commandes Bourne, vous devez donc exécuter `/bin/sh`, `/bin/bash`, `/bin/ksh` et ainsi de suite.

Voici ce que vous obtenez en exécutant les commandes précédentes sur les distributions prises en charge par Tealeaf.

Remarque : Le RPM tealeaf-pca effectue l'installation sur une installation minimale de Red Hat Enterprise Linux sans avoir besoin d'aucun autre pack. En pratique, il peut avoir besoin de packs supplémentaires.

L'installation du RPM 32 bits de Tealeaf sur un système Linux 64 bits nécessite en général l'installation de bibliothèques 32 bits supplémentaires.

- Voir Chapitre 2, «Installation», à la page 17.

Remarque : Le pack fournissant la capacité nécessaire au pack de Tealeaf peut différer entre les distributions et les différentes versions et mises à jour d'une même distribution.

Pour plus d'informations sur les packs nécessaires en fonction des versions spécifiques du système d'exploitation, voir Chapitre 2, «Installation», à la page 17.

Quelles modifications le RPM tealeaf-pca effectue-t-il sur le serveur de la PCA ?

Question

Quelles modifications le RPM tealeaf-pca effectue-t-il sur le serveur d'IBM Tealeaf Application de capture passive CX ?

Réponse

Vous pouvez installer Passive Capture dans un répertoire différent de celui par défaut, `/usr/local/ctccap`.

- Voir «Comment effectuer l'installation dans un autre répertoire que celui défini par défaut ?», à la page 270.

Le pack créé le répertoire de fichiers journaux `/var/log/tealeaf` par défaut, si celui-ci n'existe pas déjà. Il s'agissait de `/usr/local/ctccap/logs` dans les versions précédentes.

- Lorsque vous mettez à niveau une installation antérieure qui contient un répertoire `/usr/local/ctccap/logs` qui n'est pas vide, le pack utilise le répertoire `/usr/local/ctccap/logs` existant au lieu de `/var/log/tealeaf`. Ce comportement a pour objectif d'éviter de surprendre l'utilisateur en laissant les anciens fichiers journaux dans l'ancien répertoire (`/usr/local/ctccap/logs`) et en écrivant les nouveaux dans le nouveau répertoire (`/var/log/tealeaf`) par défaut.
- Cette recherche du répertoire `/usr/local/ctccap/logs` est indépendante du préfixe d'installation choisi pour la mise à niveau de l'installation. Donc, si vous

installez Passive Capture dans `/opt/tealeaf`, le pack recherche toujours un répertoire `/usr/local/ctccap/logs` non vide.

Le pack exécute les opérations suivantes sur les fichiers :

- Crée les certificats autosignés SSL suivants dans `/usr/local/ctccap/etc`. Le pack les crée automatiquement pour faciliter les installations qui ne fournissent pas leurs propres certificats SSL :

  ```
  /usr/local/ctccap/etc/tealeaf-pca.crt
  /usr/local/ctccap/etc/tealeaf-pca.key
  /usr/local/ctccap/etc/tealeaf-tts.crt
  /usr/local/ctccap/etc/tealeaf-tts.key
  /usr/local/ctccap/etc/tealeaf-tts.pem
  /usr/local/ctccap/etc/tealeaf-web.crt
  /usr/local/ctccap/etc/tealeaf-web.key
  ```

  Remarques :
  - Les fichiers tealeaf-pca sont inutilisés pour l'instant et réservés pour une utilisation future.
  - Les fichiers tealeaf-web sont utilisés par le fichier `httpd.conf` par défaut pour la console Web.
  - Les fichiers tealeaf-tts sont fournis pour faciliter la configuration des connexions SSL avec le service de transport TeaLeaf.
  - Il est normalement possible pour l'utilisateur racine et pour celui qui effectue les captures d'écrire dans le répertoire `/usr/local/ctccap/etc`, `ctccap`.
- Installez le fichier crontab : `/etc/cron.d/tealeaf`. Le fichier crontab planifie l'exécution de `tealeaf cron` en tant qu'utilisateur `racine`.
- Installez les scripts d'initialisation suivants dans `/etc/init.d` : `tealeaf-pca`, `tealeaf-startup`.
- Créez le fichier `capture.log` dans le répertoire de `fichiers journaux` si celui-ci n'existe pas déjà.

Le pack effectue les actions suivantes afin de modifier les répertoires et les fichiers à l'extérieur du préfixe d'installation :

- Créer le groupe ctccap s'il n'existe pas déjà.
- Créer l'utilisateur ctccap s'il n'existe pas déjà.

  Remarque : Cet utilisateur est créé sans mot de passe attribué, vous ne pouvez donc pas vous connecter avec ce compte par défaut. Les risques concernant la sécurité sont minimes ; l'utilisateur ctccap peut seulement démarrer et détenir les processus Tealeaf. Selon les conditions de sécurité de votre entreprise, vous pouvez attribuer un mot de passe à l'utilisateur ctccap en vous connectant en tant qu'utilisateur racine.
- Paramétrez `/usr/local/ctccap/bin/listend` et `/usr/local/ctccap/bin-debug/listend` en tant que bit ID d'utilisateur racine (obligatoire pour que listend puisse ouvrir les périphériques eth pour le reniflement de paquets ; passez ensuite en utilisateur ctccap après avoir ouvert les périphériques eth).
- Supprimez les fichiers de la session PHP dans `/tmp`. Ceux-ci sont supposés être des fichiers de la session PHP pour la console Web de Passive Capture.
- Mettez à jour `/etc/syslog.conf` (si nécessaire) pour vous assurer qu'il contient une entrée pour la fonction local0 dans le fichier `capture.log` du répertoire de `fichiers journaux`.
- Redémarrez syslogd afin de recharger sa configuration et d'utiliser toutes les modifications apportées au fichier `/etc/syslog.conf`.

Références

- Chapitre 2, «Installation», à la page 17

Comment définir le répertoire pour le lien symbolique de tealeaf ?

Question

Comment définir le répertoire pour le lien symbolique de tealeaf ?

Réponse

Le pack tealeaf-pca crée par défaut un lien symbolique à partir de `/usr/local/bin/tealeaf` vers `/usr/local/ctccap/bin/tealeaf`.

Vous pouvez définir pour le lien symbolique un autre répertoire que `/usr/local/bin` en paramétrant la variable d'environnement `TEALEAFCMDDIR`. Il doit s'agir du nom complet d'un répertoire. Vous devez paramétrer la variable d'environnement avant de commencer l'installation du RPM et la mise à niveau des commandes ainsi que du script `tpcinstaller.sh`.

Voici un exemple de commande qui définit un emplacement différent pour l'installation du lien symbolique :

```
env TEALEAFCMDDIR=/usr/bin rpm -U tealeaf-pca-3204-1.RHEL4.i386.rpm
```

Comment désactiver la création d'un lien symbolique tealeaf ?

Question

Comment désactiver la création d'un lien symbolique tealeaf ?

Réponse

Par défaut, le pack tealeaf-pca crée un lien symbolique qui conduit à la commande `/usr/local/ctccap/bin/tealeaf`.

Vous pouvez désactiver la création de ce lien en paramétrant la variable d'environnement `TEALEAFCMDENABLE` sur `NO`. Vous devez paramétrer la variable d'environnement avant de commencer l'installation du RPM et aussi mettre à niveau les commandes et le script `tpcinstaller.sh`.

Voici un exemple d'appel permettant de désactiver la création du lien symbolique.

```
env TEALEAFCMDENABLE=NO rpm -U tealeaf-pca-3204-1.RHEL4.i386.rpm
```

Comment effectuer l'installation dans un autre répertoire que celui défini par défaut ?

Question

Comment effectuer l'installation dans un autre répertoire que `/usr/local/ctccap` ?

Réponse

Remarque : Cette solution nécessite la version de `tpcinstaller.sh` du 05/07/2005, Révision 17, ou une version ultérieure.

Vous pouvez définir pour le pack tealeaf-pca un autre répertoire que celui par défaut, à savoir `/usr/local/ctccap`. Vous pouvez définir l'autre répertoire à l'aide des options de commandes `--prefix` ainsi qu'avec les commandes d'installation et de mise à niveau.

Voici quelques exemples de commandes RPM :

```
rpm -i --prefix=/opt/tealeaf tealeaf-pca-3204-1.RHEL4.i386.rpm
rpm -U --prefix=/home/tealeaf tealeaf-pca-3204-1.RHEL4.i386.rpm
```

Si vous n'utilisez pas l'option `--prefix` pendant une installation ou une mise à niveau, le RPM utilise le répertoire d'installation par défaut défini dans le fichier du pack tealeaf-pca, à savoir `/usr/local/ctccap`. Une fois que vous avez changé un pack d'emplacement, vous devez constamment définir l'autre répertoire pour que le paquet puisse chercher les installations précédentes et qu'il puisse les mettre à jour.

Si vous utilisez le script d'installation, `tpcinstaller.sh`, vous pouvez définir la variable d'environnement `TPCINSTALLPREFIX` avant de démarrer le script d'installation du pack tealeaf-pca.

Si vous ne définissez pas la variable d'environnement `TPCINSTALLPREFIX` avant de démarrer le script, celui-ci détermine le préfixe d'installation actuel et le transmet automatiquement aux commandes RPM qu'il exécute. Si le pack n'est pas déjà installé ou s'il s'agit d'une version qui ne peut pas être déplacée, tealeaf-pca utilise le répertoire par défaut, `/usr/local/ctccap`.

Voici un exemple de commande du script `tpcinstaller.sh`.

```
env TPCINSTALLPREFIX=/opt/tealeaf /etc/opt/tpcinstaller.sh \
  tealeaf-pca-3204-1.RHEL3-i386.rpm
```

Quels répertoires et quels fichiers ne se situent pas dans le répertoire d'installation ?

Question

Quels répertoires et quels fichiers ne se situent dans le répertoire d'installation ?

Réponse

Remarque : Cette solution nécessite la version de `tpcinstaller.sh` du 05/07/2005, Révision 17, ou une version ultérieure.

La liste suivante énumère les répertoires et fichiers associés à Passive Capture qui ne se trouvent pas dans le répertoire d'installation, qui est, par défaut, `/usr/local/ctccap`. Le logiciel utilise certains chemins directement. Certains peuvent être configurés par l'utilisateur et d'autres sont gérés dans les conditions normales d'administration et d'utilisation du logiciel.

/archive [facultatif]

La procédure d'installation minimale de Red Hat Enterprise Linux fait référence au répertoire facultatif. Celui-ci existe au cas où il faudrait activer l'archivage des paquets pour diagnostiquer différentes anomalies relatives à la capture. Il n'est pas nécessaire pour l'exploitation normale et n'est pas utilisé par défaut.

/etc/cron.d/tealeaf

Le pack tealeaf-pca permet l'installation de crontab afin qu'il puisse s'en servir.

```
/etc/init.d/tealeaf-pca.sh
/etc/init.d/tealeaf-startup.sh
```

Le pack tealeaf-pca permet l'installation des scripts `tealeaf-pca.sh` et `tealeaf-startup.sh` pour contrôler le démarrage et l'arrêt du logiciel.

/etc/opt/tealeaf

Passive Capture utilise ce répertoire pour différents paramètres de configuration et d'installation. Par exemple, tealeaf-pca utilise ce répertoire afin d'enregistrer le répertoire d'installation dans le fichier `/etc/opt/tealeaf/config/installprefix` et l'emplacement du lien symbolique de tealeaf dans le fichier `/etc/opt/tealeaf/config/tealeafcmd`. Le script `tpcinstaller.sh` utilise ce répertoire pour ses fichiers de configuration, y compris les clés SSL qui doivent être importées automatiquement.

/etc/syslog.conf

Passive Capture utilise la fonction syslog pour consigner des messages qui sont configurés dans ce fichier.

`/etc/group`, `/etc/passwd`, ainsi que d'autres fichiers relatifs au compte utilisateur.

S'ils n'existent pas déjà, le pack tealeaf-pca crée un compte utilisateur et un compte groupe afin d'exécuter le logiciel. Ces opérations modifient plusieurs des fichiers système mis à jour lors de la création ou la mise à jour de comptes utilisateurs.

```
/tmp/tealeaf-pca-11-prein.log
/tmp/tealeaf-pca-12-postin.log
/tmp/tealeaf-pca-21-preun.log
/tmp/tealeaf-pca-22-postun.log
```

Tealeaf-pca crée les fichiers journaux afin d'enregistrer plusieurs activités relatives à l'installation.

/tmp/tealeaf-pca.log

Le pack tealeaf-pca, pour les builds antérieures à 3204, utilisait le fichier journal pour enregistrer plusieurs activités relatives à l'installation.

/tmp/tpcinstaller.log

Le script `tpcinstaller.sh` utilise le fichier journal pour enregistrer ses activités.

/usr/local/bin/tealeaf

Le fichier ci-dessus est un lien symbolique vers la commande Tealeaf dans le sous-répertoire bin du répertoire d'installation. Par exemple: `/usr/local/ctccap/bin/tealeaf`. Les variables d'environnement `TEALEAFCMDDIR` et `TEALEAFCMDENABLE` gèrent l'emplacement et la création de ce lien symbolique.

/var/log/messages

Passive Capture utilise la fonction syslog pour consigner des messages qui peuvent affecter le fichier journal, ceux-ci sont configurés dans `/etc/syslog.conf`.

/var/log/tealeaf

Passive Capture utilise ce répertoire pour ses fichiers journaux.

Comment retirer le système de chiffrement Diffie-Hellman de la liste des chiffrements SSL de serveur Web ?

Diffie-Hellman est un type de chiffrement SSL. Il est destiné aux logiciels tiers qui sont des systèmes autres que les systèmes situés aux deux extrémités d'une conversation et qui ne peuvent pas déchiffrer le trafic des communications. Les sessions utilisateur établies avec un serveur Web à l'aide de ce système de chiffrement ne peuvent pas être capturées par IBM Tealeaf Application de capture passive CX.

Par défaut, les versions plus récentes du navigateur Firefox essaient de négocier en faveur de la famille de systèmes de chiffrement Diffie-Hellman. A cause de la popularité grandissante de Firefox, Tealeaf fournit à nos clients les instructions suivantes sur la manière de désactiver la négociation Diffie-Hellman sur leurs serveurs Web, s'ils le souhaitent.

Remarque : Si l'infrastructure du serveur Web comprend un périphérique d'interruption ou d'accélération du SSL plus en amont et plus proche du serveur Web du visiteur que de l'endroit où le serveur d'IBM Tealeaf Application de capture passive CX contrôle le trafic (serveur de la PCA), alors le serveur de la PCA peut voir tout le trafic en texte brut non-SSL, même si le système Diffie-Hellman s'applique. Dans ce cas, la solution suivante ne s'applique pas. Le périphérique d'interruption du SSL peut négocier librement le système Diffie-Hellman avec le navigateur du visiteur. Ceci est dû au fait que le serveur de la PCA se situe en aval du trafic chiffré et qu'il n'a à faire aucun chiffrement.

Choix de l'emplacement des serveurs à l'aide du système Diffie-Hellman

Dans un environnement d'application Web constitué de nombreux serveurs, l'emplacement des serveurs utilisant le système de chiffrement Diffie-Hellman ne peut pas être choisi au hasard.

Grâce à Wireshark, vous pouvez appliquer un filtre d'affichage afin d'affiner la liste des serveurs et d'identifier ceux qui utilisent le système de chiffrement Diffie-Hellman.

- Pour plus d'informations sur Wireshark, rendez-vous sur `http://www.wireshark.org`.

1. Démarrez Wireshark.
2. Chargez ou capturez un fichier TCPdump du trafic soumis à la PCA.
3. Dans la zone de saisie **Filtre**, copiez la chaîne suivante. Modifiez-la en retirant les barres obliques inversées à la fin de chaque ligne, celles-ci étant utilisées pour le prolongement du signal. Ensuite, collez la chaîne afin de filtre le trafic wireshark.

```
ssl.handshake.ciphersuite == 0x10 || ssl.handshake.ciphersuite == 0x1a || \
ssl.handshake.ciphersuite == 0x1b || ssl.handshake.ciphersuite == 0x30 \
||ssl.handshake.ciphersuite == 0x31 || ssl.handshake.ciphersuite == 0x32 || \
ssl.handshake.ciphersuite == 0x33 || ssl.handshake.ciphersuite == 0x34 \
||ssl.handshake.ciphersuite == 0x36 || ssl.handshake.ciphersuite == 0x37 || \
ssl.handshake.ciphersuite == 0x38 || ssl.handshake.ciphersuite == \
0x39||ssl.handshake.ciphersuite == 0x3a || ssl.handshake.ciphersuite == 0x63 \
|| ssl.handshake.ciphersuite == 0x65 || ssl.handshake.ciphersuite == 0x66
```

4. Le filtre du trafic n'affiche désormais que le trafic des systèmes de chiffrement Diffie-Hellman.
5. L'utilisation du système de chiffrement Diffie-Hellman doit être désactivée sur le ou les serveurs répertoriés. Pour plus d'informations, effectuez les étapes suivantes selon le type de serveur.

Désactivation

Pour désactiver la suite de chiffrement Diffie-Hellman à partir de votre serveur Web, choisissez l'une des options suivantes. Si votre serveur Web n'est pas répertorié, reportez-vous à sa documentation pour les instructions à suivre afin de désactiver cette suite de chiffrement pour votre serveur Web.

Désactivation du système de chiffrement Diffie-Hellman sur des serveurs IIS

1. Ajoutez ou modifiez la clé de registre sur chaque serveur Web :

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\
SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman\
Enabled = 0 (DWORD value)
```

2. Redémarrez le serveur Web pour que les modifications prennent effet.

Désactivation du système de chiffrement Diffie-Hellman sur des serveurs Apache

Sur chaque serveur Web, dans le fichier `ssl.conf` ou, dans certains cas, dans le fichier principal de configuration d'Apache, ajoutez l'identificateur `!DH:` au début de la chaîne d'options de configuration SSLCipherSuite.

1. Dans le répertoire de configuration d'Apache recherchez le fichier :
   `ssl.conf`
   ou
   `httpd.conf`
2. Recherchez le mot clé SSLCipherSuite, dont la valeur de chaîne doit ressembler à ce qui suit :

   ```
   "ALL:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP"
   ```

3. Ajoutez `!DH:` après la liste `ALL:` afin que la ligne soit comme suit :

   ```
   "ALL:!DH:!ADH:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP"
   ```

   Remarque : La chaîne `!ADH:` est désormais redondante et peut être supprimée de la chaîne.
4. Si vous n'utilisez pas une section globale, effectuez à nouveau cette modification dans chaque section de configuration du SSL.
5. Enregistrez le fichier.
6. Redémarrez le serveur Web pour que les modifications prennent effet.

Certains hits SSL n'apparaissent pas dans les sessions de navigation de Firefox

Remarque : Ce problème est résolu dans la build 3611 PCA et ultérieure.

Remarque : A partir de la build 3327, IBM Tealeaf Application de capture passive CX prend en charge l'extension SSL TLSv1 de tickets de session. Si vous utilisez la build 3327 ou une build ultérieure et que cette extension est activée sur votre serveur Web, la PCA peut capturer toutes les données de session correctement.

- Si la build que vous utilisez est antérieure à 3327, vous devez la mettre à jour pour obtenir la dernière version au lieu d'utiliser cette solution de contournement.
- A partir de la build PCA 3611, la PCA peut capturer du trafic SSL TLSv1.1. Cette explication s'applique aussi à TLSv1.1 pour les versions qui le prennent en charge. Pour plus d'informations sur le téléchargement d'IBM Tealeaf , reportez-vous à IBM Passport Advantage Online.

Quand les sessions sont lancées par le navigateur Firefox 3 puis reprises plus tard, les hits SSL ne sont pas déchiffrés. Ils disparaissent donc du trafic capturé.

- Ce problème n'est pas affiché sur le trafic non SSL.
- Ce problème n'est pas connu ou affiché sur un autre navigateur que Firefox 3.

Il se produit à cause d'une fonctionnalité d'extension SSL installée dans la version 3 de Firefox et dans les modules OpenSSL qui utilisent les serveurs Web Apache les plus récents (et probablement d'autres serveurs Web). Une nouvelle extension du protocole SSL TLSv1 (RFC-5077) connue sous le nom d'extension de tickets de session, qui permet la reprise d'une session sans état, chiffre les informations d'état SSL utilisées uniquement lorsque le navigateur client et le serveur Web respectent tous les deux les normes.

Tealeaf ne prend pas en charge cette fonctionnalité d'extension SSL. Si vous avez installé ou mis à niveau la dernière build du serveur Apache V2.2 au cours des mois, cette nouvelle extension a sûrement des répercussions sur votre installation. Les instructions suivantes vous sont fournies pour vous permettre de désactiver cette extension dans Apache.

Remarque : Vous devez désactiver cette fonctionnalité dans vos serveurs Web.

Symptômes

Si des visiteurs de votre application Web utilisent le protocole SSL via Firefox 3 et qu'ils quittent ensuite leur session, les hits ne seront pas capturés par la PCA une fois que la session reprendra. Ceci est dû au fait que Firefox 3 prend en charge cette nouvelle extension SSL par défaut.

Si Firefox négocie l'établissement d'une liaison SSL avec votre serveur Web pour reprendre la session, le navigateur s'attendra à ce que le serveur fournisse un identifiant unique SSL 32 bits au navigateur client.

- Le but de cette fonctionnalité est de réutiliser les informations sur les clés des sessions SSL et de réduire l'utilisation du protocole SSL dans les sessions SSL ultérieures.

Tealeaf ne prenant pas en charge cette extension SSL, il ne reconnaît pas cet identifiant SSL 32 bits. Sans cet identifiant, le logiciel Tealeaf PCA ne peut déchiffrer aucun trafic supplémentaire à l'aide de l'identifiant dans les sessions SSL qui ont repris.

Dans les exemples suivants, vous pouvez voir la manière dont les identifiants de session sont distribués au visiteur qui rouvre une session dans Firefox 3 par opposition à Internet Explorer.

Pour Firefox :

```
SSL cipher used: Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Session ID Length: 0
```

Pour IE :

```
SSL cipher used: Cipher Suite: TLS_RSA_WITH_RC4_128_MD5 (0x0004)
Session ID Length: 32
Session ID: 2FD9AAAEE999B2EA3DEF8FA005CD0CDD3D6EAE62E05E4975...
```

Comme vous pouvez le voir plus haut, la longueur de l'identifiant de session SSL est de 0, il ne fournit donc aucune valeur utilisable.

Cette nouvelle extension de protocole SSL TLSv1 qui permet une reprise de session sans état, connue sous le nom d'extension de tickets de session, chiffre les informations d'état SSL comme par exemple l'identifiant de session SSL dans un pack "ticket" que le navigateur client et le serveur doivent tous deux utiliser.

Actuellement, Firefox 3 est le seul navigateur à utiliser cette extension par défaut. Pour que cette extension soit acceptée, le serveur doit lui aussi la prendre en charge.

A tester

Pour voir si le problème se produit ou pas, vous pouvez forcer votre serveur Web ou votre proxy Web à utiliser le système de chiffrement choisi par IE afin de voir si les sessions Firefox sont capturées correctement ou pas.

A réparer

Actuellement, la seule méthode pour résoudre le problème consiste à désactiver l'utilisation de cette extension SSL sur le serveur Web ou le proxy Web.

Navigateur Firefox

Pour contourner une anomalie en utilisateur individuel, vous pouvez désactiver l'utilisation de cette extension via Firefox. Pour désactiver l'utilisation de cette extension dans Firefox, procédez comme suit :

1. Ouvrez Firefox.
2. Désactivez le chiffrement TLS 1.0 dans Firefox.
   a. Dans le menu de Firefox, sélectionnez **Outils** > **Options** > **Avancé** > **Chiffrement**.
   b. Dans la section Protocoles, désélectionnez la case **Utiliser TLS 1.0**.
   c. Cochez la case **Utiliser SSL 3.0**.
   d. Cliquez sur **OK** pour enregistrer vos modifications.
   - Pour plus d'informations, voir `https://kb.bluecoat.com/index?page=content&id=KB2887&actp=RSS`.

Proxy Web

Si votre serveur proxy gère le traitement SSL, vous pouvez désactiver l'utilisation de la fonctionnalité d'extension de tickets de session SSL TLSv1 sur le proxy. Reportez-vous à la documentation fournie avec votre serveur proxy.

Serveurs Web Apache

Selon la version d'Apache, cette fonctionnalité peut être activée par défaut. Le dernier mod_ssl d'Apache utilise la version 9.8j d'OpenSSL ou des versions plus récentes permettant l'activation de l'extension de tickets de session TLS par défaut.

- Cette fonctionnalité est très probablement apparue pour la première fois dans la version 2.2 du serveur Apache.

Pour la désactiver :

1. Sur le serveur Web, modifiez `/usr/local/apache2/conf/httpd.conf`.
2. Ajoutez le fragment suivant à l'emplacement correspondant dans le fichier :

```
SSLEngine on
SSLOptions +StrictRequire

<Directory />
    SSLRequireSSL
</Directory>

SSLProtocol +all -TLSv1 -SSLv3
SSLCipherSuite HIGH:MEDIUM:!aNULL:+SHA1:+MD5:+HIGH:+MEDIUM:!DH
```

   Remarque : Dans le passage ci-dessus, la référence `!DH` permet de supprimer l'algorithme de chiffrement Diffie-Hellman, celui-ci devant être désactivé pour toutes les solutions Tealeaf. Voir «Comment retirer le système de chiffrement Diffie-Hellman de la liste des chiffrements SSL de serveur Web ?», à la page 273.
3. Enregistrez le fichier.
4. Redémarrez le service Apache.
   - Pour plus d'informations, voir `http://www.securityfocus.com/infocus/1818`.

Serveurs Web autres que les serveurs Apache

La plupart des serveurs Web ne proposent pas de méthode simple pour désactiver l'emploi de cette extension. Vous pouvez la désactiver en désactivant l'emploi du protocole TLS 1.0 à l'aide des options de configuration du serveur Web. Pour obtenir des informations plus détaillées, consultez la documentation du produit.

Comment définir d'autres fichiers de configuration ?

Question

Comment définir d'autres fichiers de configuration ?

Réponse

Vous pouvez utiliser le script `tpcinstaller.sh` pour écraser automatiquement différentes configurations créées par le pack tealeaf-pca lorsque vous l'avez installé au départ.

Ces fichiers de configuration sont normalement créés lorsqu'ils n'existent pas déjà. Une fois qu'ils existent, le pack tealeaf-pca ne les modifie pas et ne les met pas à jour. Si ce pack remarque que vous n'avez pas modifié les fichiers, il les supprime durant la désinstallation.

Utilisez la commande `postinstall` du script `tpcinstaller.sh` pour écraser plusieurs fichiers de configuration. Après l'installation, le script se trouve dans le sous-répertoire `bin` du répertoire d'installation.

Le script permet une installation et une configuration automatiques mais cet exemple ne fait qu'illustrer les effets de sa commande `postinstall` qui permet d'écraser les fichiers de configuration puis de démarrer le logiciel. Voici un exemple succinct illustrant l'essence de ses capacités de base.

- Cet exemple présuppose que le pack tealeaf-pca est déjà installé dans le répertoire `/opt/tealeaf`.
- Les commandes à exécuter en tant qu'utilisateur racine sont précédées d'un signe dièse (#).

1. Initialisez le répertoire `/etc/opt/tealeaf` :

   ```
   # sh /opt/tealeaf/bin/tpcinstaller.sh init
   ```

2. Créez et/ou placez les fichiers de configuration personnalisés dans le répertoire `/etc/opt/tealeaf` créé à l'étape 1.
   a. Pour écraser `ctc-conf.xml`, procurez le fichier `ctc-conf-custom.xml`. Si vous souhaitez que le script d'installation convertisse automatiquement des fichiers PEM en fichiers PTL et qu'il mette à jour le fichier `ctc-conf.xml` avant l'écrasement :
      1) Mettez vos fichiers dans `/etc/opt/tealeaf/capturekeys`.
      2) Remplacez la section `<CaptureKeys>` de `ctc-conf-custom.xml` par :

         ```
         <CaptureKeys>CAPTUREKEYSCONF</CaptureKeys>
         ```

   b. Pour écraser `httpd.conf`, procurez le fichier `httpd-custom.conf`.
   c. Pour écraser `privacy.cfg`, procurez le fichier `privacy-custom.cfg`.
   d. Pour écraser `runtime.conf`, procurez le fichier `runtime-custom.conf`.
3. Créez un fichier de configuration qui ordonne au script d'installation de toujours écraser les fichiers de configuration au lieu de ne les écraser que lorsqu'aucune modification ne leur a été apportée par rapport aux fichiers par défaut. Vous trouverez ci-dessous le contenu d'un tel script, qui doit être intitulé `/etc/opt/tealeaf/tpcinstaller.conf` :

   ```
   custom_capture_conf_enable="YES"
   custom_httpd_conf_enable="YES"
   custom_privacy_conf_enable="YES"
   custom_runtime_conf_enable="YES"
   ```

4. Ecrasez les fichiers de configuration et démarrez tous les services :

   ```
   # sh /etc/opt/tealeaf/bin/tpcinstaller.sh postinstall
   ```

   Si vous voulez aussi ordonner au script d'installation d'installer/mettre à jour le RPM, vous devez alors en enregistrer une copie dans `/etc/opt/tealeaf` puis le démarrer avec le nom du fichier RPM. Exemple :

```
# env TPCINSTALLPREFIX=/opt/tealeaf sh /etc/opt/tealeaf/tpcinstaller.sh \
/root/tealeaf-pca-3204-1.RHEL4.i386.rpm
```

Remarque : L'utilisation de `TPCINSTALLPREFIX` nécessite au minimum l'installation de la version 3204 de la PCA.

Pourquoi la console Web de la PCA ignore-t-elle les modifications que j'ai enregistrées ?

Question

Pourquoi la console Web de la PCA ignore-t-elle les modifications que j'ai enregistrées ?

Réponse

Vérifiez que les cookies sont activés. Pour que la console Web de la PCA conserve la session telle quelle lorsque vous effectuez plusieurs tâches, les cookies doivent être activés.

Après avoir cliqué sur **Enregistrer les modifications**, si les cookies sont désactivés, alors la page que vous passez en revue retourne à son état initial avant les modifications.

Références

- «Console Web de la PCA - Onglet Récapitulatif», à la page 60

Pourquoi est-il impossible d'interrompre les processus de la console Web ?

Question

Pourquoi est-il impossible d'interrompre les processus de la console Web ?

Réponse

Dans la build 3100, l'emplacement par défaut du fichier `httpd.pid` utilisé par le script `tealeaf` pour trouver la console Web a changé. Ce fichier se trouvait dans le `répertoire de fichiers journaux`, mais il a été déplacé dans le répertoire `/usr/local/ctccap/var` afin de contenir d'autres fonctionnalités.

Si vous aviez modifié le fichier `httpd.conf` pour qu'il soit différent de `httpd.conf.default`, votre fichier `httpd.conf` est alors préservé lorsqu'un pack tealeaf-pca plus récent installe un nouveau fichier `httpd.conf.default`. Ceci signifie que le nouveau script Tealeaf dans le pack de la version 3100 ou ultérieure ne peut pas trouver `httpd.pid` car la console Web continue d'écrire ce fichier dans l'ancien emplacement défini par `httpd.conf`.

Pour résoudre ce problème, suivez les instructions suivantes :

- Interrompez tout les processus en cours en tant qu'utilisateur racine à l'aide de la commande suivante :
  ```
  killall httpd
  ```
- Examinez les différences entre `httpd.conf` et le fichier par défaut, `httpd.conf.default`, issu du pack. Par exemple, vous pouvez voir les différences à l'aide de la commande `diff` de la manière suivante :
  ```
  cd /usr/local/ctccap/etc
  diff -c httpd.conf.default httpd.conf
  ```
- Isolez les différences effectuées localement pour le serveur de l'application Passive Capture (par exemple, authentification de base, désactivation du port non-SSL) des modifications apportées par le pack.

- Enregistrez le fichier `httpd.conf` existant, écrasez `httpd.conf` et remplacez-le pas `httpd.conf.default` puis fusionnez les modifications isolées depuis l'étape 3.

Où se trouve le répertoire de journaux ctccap ?

Question

Où se trouve le répertoire `/usr/local/ctccap/logs` ?

Réponse

Depuis la build 3102, les fichiers journaux de Passive Capture se trouvent dans le répertoire `/var/log/tealeaf`. Lorsque vous installez le pack tealeaf-pca sur un ordinateur pour la première fois, celui-ci crée et utilise `/var/log/tealeaf`.

Si vous effectuez une mise à niveau depuis une version précédente et que le répertoire `/usr/local/ctccap/logs` n'est pas vide, Passive Capture continue alors de l'utiliser à la place de `/var/log/tealeaf`.

La page Sauvegarde/Journaux de la console Web est mise à jour afin d'afficher le répertoire utilisé pour les fichiers journaux.

Comment modifier le répertoire de fichiers journaux manuellement ?

Question

Comment modifier manuellement le répertoire de fichiers journaux de `/var/log/tealeaf` à XYZ ?

Réponse

Pour les builds 3100 et ultérieures, voici le répertoire de `fichiers journaux` utilisé par de nouvelles installations :

```
/var/log/tealeaf
```

Si vous ne souhaitez pas que Passive Capture utilise ce répertoire, procédez alors comme suit. Ces instructions permettent de configurer le répertoire de `fichiers journaux` pour qu'il s'agisse de `/var/tealeaf`.

- Connectez-vous en utilisateur `racine` pour suivre ces instructions.
- Pour cela, Passive Capture doit être déjà installé dans le répertoire `/usr/local/ctccap`.

1. Interrompez tous les démons de Passive Capture :

   ```
   tealeaf stop
   tealeaf stop failoverd
   ```

2. S'il n'existe pas déjà, créez le répertoire et définissez ses conditions de propriété et d'autorisations.

   ```
   mkdir /var/tealeaf
   chmod u=rwx,go= /var/tealeaf
   chown ctccap:ctccap /var/tealeaf
   ```

   Une longue liste répertoriant seulement les éléments du répertoire doit avoir pour résultat :

   ```
   # ls -ld /var/tealeaf
   drwx------    2 ctccap   ctccap       4096 Sep  6 14:41 /var/tealeaf
   ```

Remarque : Le groupe ctccap a été créé dans la build 3101.

3. Créez des fichiers journaux vides. Vous pouvez utiliser la commande tealeaf initlogs. Si celle-ci n'est pas disponible dans la version que vous exécutez, il vous faudra au moins créer le fichier capture.log à l'aide des commandes suivantes :

```
touch /var/tealeaf/capture.log
chmod u=rw,go= /var/tealeaf/capture.log
chown ctccap:ctccap /var/tealeaf/capture.log
```

   Une longue liste répertoriant les éléments du répertoire doit avoir pour résultat :

```
# ls -l /var/tealeaf
total 0
-rw-------    1 ctccap   ctccap          0 Sep  6 14:42 capture.log
```

   Vous pouvez choisir de copier tous vos fichiers journaux existants à partir de /var/log/tealeaf vers le nouveau répertoire.

4. Modifiez le nouveau fichier de configuration du démon syslog : /etc/syslog.conf. Remplacez la ligne pour local0 :

```
local0.* -/var/log/tealeaf/capture.log
```

   par ce code :

```
local0.* -/var/tealeaf/capture.log
```

5. Redémarrez le démon syslog :

```
/etc/init.d/syslog stop
/etc/init.d/syslog start
```

   Sur les systèmes Red Hat, vous pouvez utiliser :

```
service syslog stop
service syslog start
```

6. Modifiez le fichier /usr/local/ctccap/etc/runtime.conf utilisé par Passive Capture. Supprimez toute définition de variable existante pour logfiledir et ajoutez-y la ligne suivante :

```
logfiledir="/var/tealeaf"
```

7. Démarrez les démons de Passive Capture :

```
tealeaf start failoverd
tealeaf start
```

Si vous observez /var/tealeaf/capture.log, vous devez voir des messages indiquant le démarrage de Passive Capture.

Toutes les étapes ci-dessus sont basées sur le traitement effectué pour la variable de configuration logfiledir par le script de post-installation postinstallimp.sh compris dans la distribution de Passive Capture (dans le sous-répertoire sbin).

Comment faire pour que la PCA efface automatiquement ses statistiques ?

Question

Comment faire pour que la PCA efface automatiquement ses statistiques ?

Réponse

Créez un travail cron dans /etc/cron.d/tealeaf pour réveiller les statistiques et les effacer. Exemples :

```
* * * * * root /usr/local/ctccap/bin/tealeaf cron > /dev/null 2>&1
# the command 'tealeaf cron' is run every minute (already exists in
# /etc/cron.d/tealeaf
```

```
30 3 * * * root /usr/local/ctccap/bin/tealeaf clearstats > /dev/null 2>&1
# 'tealeaf clearstats' is run at 3:30 a.m. every day.
```

```
15 4 * * 2 root /usr/local/ctccap/bin/tealeaf clearstats > /dev/null 2>&1
# 'tealeaf clearstats' is run at 4:15 a.m. on Tuesdays.
```

```
01 0 1 * * root /usr/local/ctccap/bin/tealeaf clearstats > /dev/null 2>&1
# 'tealeaf clearstats' is run at 12:01 a.m. on the first day of every month.
```

Quel est le numéro de port par défaut correspondant au basculement ?

Question

Quel est le numéro de port par défaut (ou recommandé) pour le basculement ?

Réponse

Si vous ne définissez pas de numéro de port lorsque vous configurez un basculement maître ou subordonné, le basculement utilise alors le port 9866.

Comment la PCA gère-t-elle la duplication des paquets TCP ?

Un contrôle est effectué sur les numéros de séquence TCP des paquets à l'intérieur de la connexion TCP uniquement. Les doublons sont déterminés en fonction des numéros de séquence TCP.

Même si les processus de la PCA peuvent traiter les paquets de trafic dupliqués, ceux-ci ne sont pas nécessaires et peuvent entraîner des baisses de performances si le système s'approche de son niveau maximal de performances. La meilleure chose à faire est de ne pas soumettre plus de paquets dupliqués que nécessaire à la PCA.

Au niveau du paquet TCP, IBM Tealeaf Application de capture passive CX contrôle la présence de paquets dupliqués dans une connexion TCP. La PCA le fait en évaluant leur numéro de séquence TCP. Lorsque des doublons sont détectés, ils sont gérés de la manière suivante :

- Lorsque deux paquets s'affichent dos à dos dans la même connexion, le deuxième est supprimé.
- Si deux paquets avec le même numéro de séquence s'affichent, mais qu'ils ne sont pas dos à dos, le deuxième est supprimé.
- Si les emplacements de départ et d'arrivée des paquets ne sont pas les mêmes, la PCA les accepte et les rassemble pour les délivrer aux canisters en aval.

Dans l'onglet **Statistiques** de la console Web de la PCA, vous pouvez contrôler la fréquence d'apparition des paquets TCP dupliqués. Voici la statistique clé permettant de la contrôler :

```
Total back-to-back duplicate packets
```

Dans le fichier `stats.xml`, cette statistique s'affiche de la manière suivante :

```
<TcpTotalDuplicatePackets>
```

Un nombre élevé de paquets dupliqués peut indiquer que les miroirs de port des commutateurs réseau ne sont pas configurés correctement. Par exemple, si le nombre de paquets dupliqués correspond à environ la moitié de la valeur définie dans la statistique `Total packets rcvd value`. Il peut aussi indiquer que les ports soumettent un trafic dupliqué au serveur IBM Tealeaf Application de capture passive CX.

voir «Statistiques par instance», à la page 137.

Comment la PCA identifie-t-elle les pages ReqCanceled ?

Cette section explique brièvement comment la PCA évalue et identifie des pages comme étant des pages ReqCancelled.

- Une page ReqCancelled peut être annulée sur demande du navigateur client (visiteur) ou du serveur Web.

Valeurs côté serveur

Une fois qu'une page de demande ou de réponse HTTP est assemblée à partir des paquets TCP, l'en-tête HTTP devient disponible. Dans l'en-tête, les valeurs calculées par le serveur pour HeaderSize et DataSize de la réponse et la demande s'affichent. Dans l'exemple suivant, la réponse brute s'affiche :

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=UTF-8
Date: Fri, 25 Feb 2011 14:40:14 GMT
Cache-Control: private
Content-Length: 83

<html>
  <body>
    Réponse
     <hr>
    Read 652 bytes in 7ms.
  </body>
</html>
```

Dans l'exemple qui précède, la valeur `Content-Length` signalée par le serveur est de 83 bits.

Valeurs calculées par la PCA

La PCA calcule aussi la taille actuelle du hit observée à partir des paquets lorsqu'ils sont rassemblés. Ces valeurs sont stockées dans la section `[env]` de la demande :

```
[env]
...
RequestHeaderSize=1741
RequestDataSize=0
RequestSize=1741
```

```
ResponseHeaderSize=418
ResponseDataSize=25151
ResponseSize=25569
...
```

Analyse des valeurs de taille du contenu

Par conséquent, la PCA utilise deux ensembles de valeurs permettant d'évaluer la taille :

- Les valeurs côté serveur
- Les valeurs observées ou calculées par la PCA

Ces nombres doivent correspondre.

Remarque : Si les valeurs observées par la PCA sont inférieures aux valeurs côté serveur insérées dans l'en-tête de réponse, la PCA marque le hit comme hit ReqCancelled.

Codage de transfert en blocs

Il existe un cas particulier où la valeur `Content-Length` n'est pas signalée par le serveur. Dans le codage de transfert en blocs, le serveur transfère des données à l'aide du protocole HTTP sans connaître à l'avance la taille totale du corps du message. Lorsque le codage de transfert en blocs est autorisé par le serveur, voici la réponse qui en résulte :

```
.HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Cache-Control: private
Pragma: no-cache
Set-Cookie: logging=CC4993FF05A9AC05B52CD9756B094B10|egapp39p|;
  Domain=.example.com; Path=/
Set-Cookie: DealDetectorUser=true; Domain=.example.com; Expires=Thu,
  20-Feb-2031 14:39:33 GMT; Path=/
P3P: CP="CAO DSP CURa ADMa DEVa TAIa PSAa PSDa IVAi IVDi CONi OUR DELi SAMi
  OTRi BUS PHY ONL UNI PUR COM NAV INT DEM STA POL HEA PRE GOV"
Content-Type: text/html
Date: Fri, 25 Feb 2011 14:39:33 GMT
Transfer-Encoding: chunked
```

Dans l'exemple qui précède, aucune valeur n'est signalée pour `Content-Length`. Puisque la longueur du contenu n'est pas connue à l'avance, la valeur suivante est insérée :

```
Transfer-Encoding: chunked
```

Lorsque la PCA remarque que le transfert est en blocs, elle assemble les paquets dans le hit et suit la valeur `DataSize` de la page jusqu'à ce qu'elle atteigne le paquet final du bloc. Ce dernier paquet est désigné par un bloc de taille nulle (la taille du bloc est codée comme suit : `0`) et ne contient aucune section de données.

Remarque : Puisque le serveur ne signale pas de valeur pour `Content-Length` dans le codage de transfert en blocs, l'en-tête de chaque bloc contient une entrée indiquant sa taille. Par conséquent, la longueur totale réelle du bloc est calculée de façon dynamique.

- Si un bloc ne parvient pas à fournir toutes ses données comme elles sont spécifiées dans son en-tête, la PCA marque la page dans lequel il apparaît comme une page ReqCancelled.

Identification des hits ReqCancelled dans Tealeaf

Voici une présentation de la manière d'identifier les hits ReqCancelled dans Tealeaf.

Données enregistrées

Lorsqu'un hit est identifié comme contenant une demande annulée, IBM Tealeaf Application de capture passive CX insère les informations suivantes dans la section `[env]` :

- Demande annulée par le visiteur (navigateur client) :

```
[env]
?
ReqCancelled=Client
?
```

- Requête annulée par le serveur :

```
[env]
?
ReqCancelled=Server
?
```

Code du statut HTTP

Le code du statut HTTP est créé en tant que partie de la réponse HTTP. Le code de statut pour un hit ReqCancelled dépend du moment où le hit a été annulé :

Moment où l'annulation s'est produite :
Valeur(s) du code de statut

Avant que le serveur envoie une réponse
Code de statut =

Une fois que le serveur a envoyé une réponse
Valeur autre que 200 (OK)

Autres caractéristiques

Selon le moment où la demande a été annulée et la manière dont elle a été annulée, certaines parties des données du hit peuvent être malformées :

- En ce qui concerne les hits soumis par IBM Tealeaf Capture d'interface utilisateur CX pour AJAX, la section `[xml1]` peut être déformée ou incomplète si le POST a été interrompu avant la fin.
- Si elle est comprise dans les éléments à capturer par la PCA, une version incomplète ou déformée de la section `[RawRequest]` peut indiquer que la demande a été annulée avant que le serveur entame le traitement de la réponse.
- En ce qui concerne les hits annulés pendant la création de la réponse, des parties de la réponse peuvent être manquantes.

Remarque : Qu'il s'agisse d'un hit dont la demande a été annulée ou au contraire d'un hit entièrement traité, la zone de l'en-tête de requête HTTP est toujours incluse. La PCA ne capture pas un hit si son en-tête de demande est manquant.

Création d'un événement

Tealeaf fournit un événement bloc de construction qui permet de détecter la présence d'un hit ReqCancelled : `Req Cancelled [BB-NoDim]`. En tant qu'événement bloc de construction, il est impossible de le chercher.

Voici quelques instructions générales à suivre pour créer l'objet d'événement permettant de suivre les hits request canceled :

1. Connectez-vous au portail en tant qu'administrateur.

2. Dans le menu du portail, sélectionnez **Configurer** > **Gestionnaire d'événements**.
3. Le gestionnaire d'événements de Tealeaf s'affiche. Voir le chapitre sur le gestionnaire d'événements Tealeaf dans le document *IBM Tealeaf Event Manager Manual*.
4. Cliquez sur l'onglet **Evénements**.
5. Cliquez sur **Nouvel événement...**. L'assistant **Ajouter un événement** s'affiche.
6. Configurez les propriétés suivantes :

   Propriété
   : **Description**

   Nom
   : Suggérez `Req Cancelled Type`.

   Description
   : Suggérez `Type of canceled request: client or server`.

   Evaluer
   : Définissez sur `Every Hit`

   Suivre
   : Définissez sur `First Per Session`, même si c'est pour un hit.

   Type de valeur
   : Définissez sur `Text`

7. Gardez pour le reste les valeurs par défaut. Cliquez sur **Condition**.
   a. Sur le panneau de gauche, cliquez sur la catégorie **Evénements**.
   b. Cliquez sur `Tealeaf Standard Events`.
   c. Sélectionnez `ReqCancelled [BB-NoDim]`. L'événement s'ajoute en tant que condition à votre définition de l'événement `Req Canceled Type`.
      1) Dans le premier menu déroulant dans la condition d'événement ajoutée, sélectionnez `Value`.
      2) Dans le menu déroulant de l'opérateur de condition, sélectionnez `Equals`.
      3) Dans la troisième zone de saisie, entrez `server`.
      4) Laissez la case sensible à la casse désélectionnée.
   d. Dans le panneau de gauche, sélectionnez à nouveau `ReqCancelled [BB-NoDim]`.
      1) Remplissez-le comme dans l'exemple ci-dessus à l'exception de la troisième zone de texte où vous devez entrer `client`.
   e. Dans le menu déroulant qui se trouve en haut du panneau principal de configuration, sélectionnez :

      ```
      Any of the following conditions must be met
      ```
   f. L'étape Condition est configurée pour contrôler la présence de toute condition d'événement. L'écran qui s'affiche doit ressembler à ça :

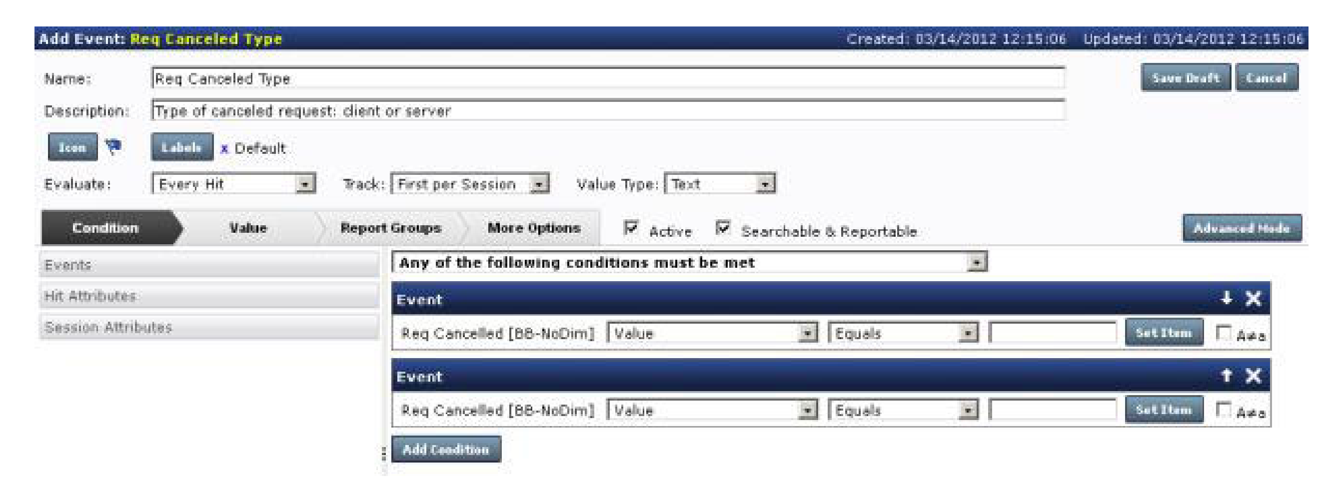


Figure 46. Evénement de type Requête annulée - Etape Condition

8. Cliquez sur l'onglet **Valeur**.
   a. Cliquez sur **Sélectionnez un article à enregistrer...**.
   b. Dans la boîte de dialogue de sélection d'un article, cliquez sur la catégorie **Evénements**.
   c. Cliquez sur **Tealeaf Standard Events**.
   d. Sélectionnez `Req Cancelled [BB-NoDim]`.
   e. Laissez la valeur du menu déroulant sur `Value`.
   f. La valeur à enregistrer est configurée de manière à être la valeur de `Req Cancelled [BB-NoDim]` définie sur `server` ou `client` si l'une ou l'autre de ces conditions est respectée. L'écran qui s'affiche doit ressembler à ça :



Figure 47. Evénement de type Requête annulée - Etape Valeur

9. Vous devez configurer les autres étapes de la définition de l'événement comme le requiert votre environnement.
10. Cliquez sur **Enregistrer le brouillon**.
11. Dans l'onglet Evénements, cliquez sur **Enregistrer les modifications** pour que le nouvel événement s'applique à votre serveur.

Recherche de sessions avec ReqCancelled Type

L'événement mentionné ci-dessus est désormais défini pour enregistrer la valeur `client` ou `serveur` si une demande est annulée par le visiteur ou le serveur Web. Vous pouvez chercher des occurrences de cet événement à l'aide du portail.

Remarque : Une fois l'événement enregistré sur le serveur, il est actif et traité sur chaque hit. Cela peut prendre du temps avant que Tealeaf ne capture et traite les sessions avec des demandes annulées.

Pour rechercher l'événement `ReqCancelled Type` suivez les instructions ci-dessous :

1. Dans le portail, sélectionnez **Rechercher** > **Sessions terminées**.
2. Pour rechercher une occurrence de hit ReqCancelled dans une session :
   a. Effacez tous les termes de recherche par défaut.
   b. Cliquez sur le terme **Evénements**.
   c. Cliquez sur **<sélectionnez un événement**.
   d. Dans **Sélecteur d'événement**, désélectionnez la case Affichage par libellés.
   e. Dans la zone de recherche, saisissez `Requête annulée`.
   f. Sélectionnez `Req Canceled Type`.
   g. Cliquez sur **Sélectionner**.
   h. Votre recherche pour savoir si l'événement existe dans une session s'affiche. L'écran qui s'affiche doit ressembler à ça :

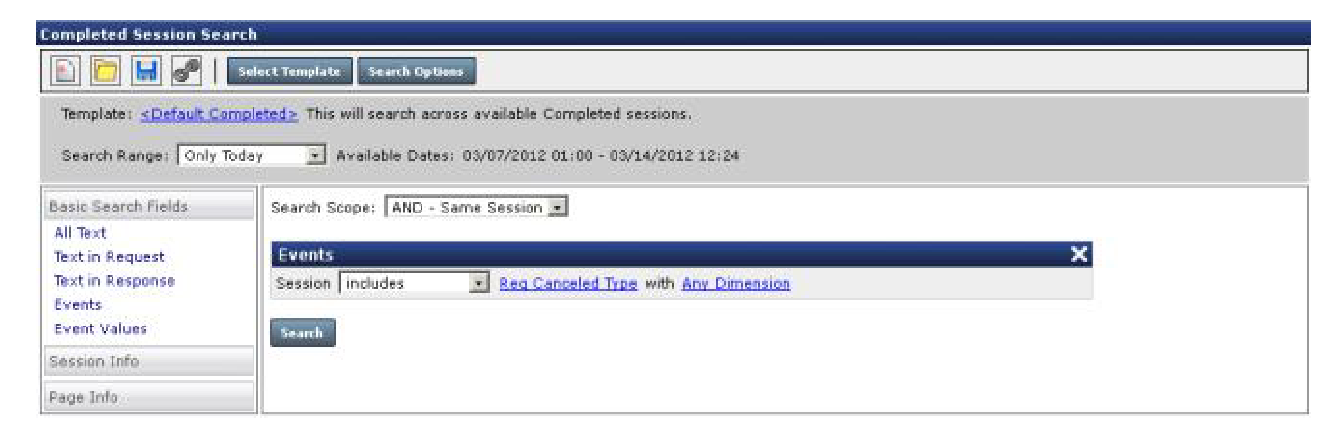


Figure 48. Req Canceled Type - Recherche de l'existence de l'événement

3. Pour rechercher le type spécifique de hit ReqCancelled dans une session :
   a. Effacez tous les termes de recherche par défaut.
   b. Cliquez sur le terme **Valeurs d'événements**.
   c. Cliquez sur **<sélectionnez un événement**>.
   d. Dans **Sélecteur d'événement**, désélectionnez la case **Affichage par libellés**.
   e. Dans la zone **Rechercher**, saisissez `Req Canceled`.
   f. Sélectionnez `Req Canceled Type`.
   g. Cliquez sur **Sélectionner**.
   h. Dans les critères de recherche, vérifiez que l'opérateur de recherche est réglé sur `Includes`.
   i. Dans la zone de saisie, entrez les valeurs suivantes :
      - `server` - recherche les hits ReqCancelled créés par le serveur
      - `client` - recherche les hits ReqCancelled créés par le client
   j. Votre recherche d'un type spécifique de hits ReqCancelled dans une session s'affiche. L'écran qui s'affiche doit ressembler à ça :

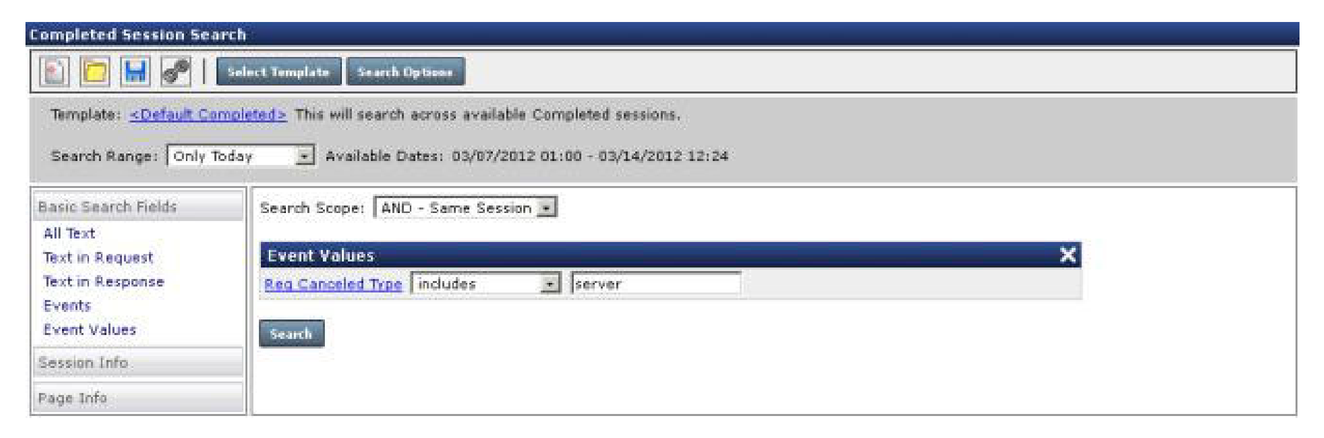


Figure 49. Req Canceled Type - Recherche de hits ReqCancelled créés par le serveur

4. Pour lancer une recherche, cliquez sur **Rechercher**.
5. Dans la liste des sessions, vous pouvez en sélectionner une à examiner pour obtenir plus d'informations. Si les sessions reprennent, vous pouvez rechercher le hit à l'endroit où la demande a été annulée à l'aide des méthodes générales suivantes :
   - Testeur d'événements : à partir de la liste des sessions, vous pouvez envoyer la session au testeur d'événements. Dans le testeur d'événements, sélectionnez l'événement `Req Canceled Type` pour qu'il s'affiche. Grâce aux résultats du test, vous pouvez rechercher le hit à l'endroit où l'événement s'est produit.
   - Voir "Envoi au testeur d'événement" dans le manuel d'utilisation d'*IBM Tealeaf cxImpact*.
   - QuickView : dans la liste des sessions, vous pouvez ouvrir QuickView qui affiche les informations sur l'événement par hit. Dans la commande du menu déroulant, sélectionnez `Event Name`. Recherchez le hit à l'endroit où l'événement `Req Canceled Type` s'est produit.
   - Voir "QuickView" dans le guide d'utilisation d'*IBM Tealeaf cxImpact User*.

Comment la PCA gère-t-elle la capture des adresses IPv6 ?

A partir de la version 3501, IBM Tealeaf Application de capture passive CX peut être configuré pour capturer des adresses IPv6.

Remarque : L'hébergement de serveurs Tealeaf à l'aide d'adresses IPv6 n'est pas pris en charge au jour d'aujourd'hui.

Remarque : Les éditions 8.4 et ultérieures prennent en charge le traitement des adresses IPv6 à des fins de recherche, relecture et création de rapports.

Remarque : Il n'est possible d'activer la capture de la PCA que par demande. Voir «Activation de la capture d'adresses IPv6», à la page 291.

Présentation d'IPv6

Internet Protocol Version 6 (IPv6) représente la méthode de nouvelle génération permettant de définir des adresses IP. IPv4, la version précédente, autorisait les adresses 32 bits, ce qui permettait de définir 2^{32} adresses. Tous les blocs d'adresses IPv4 ont été attribués.

IPv6 accepte les adresses IP 128 bits, ce qui permet de définir 2^{128} adresses. Cet élargissement des possibilités permet l'utilisation d'adresses IP attribuées à un périphérique spécifique pour l'ensemble de périphériques connectés dont le nombre est en constante augmentation. Autres fonctionnalités :

- Une flexibilité supplémentaire dans l'attribution d'adresses
- Une efficacité dans le traitement du trafic de routage
- Suppression du besoin de convertir des adresses réseau

Bien que le protocole IPv6 soit pris en charge sur tous les principaux systèmes d'exploitation, il n'introduit pas des fonctions natives d'interopérabilité avec IPv4. En général, l'interoperabilité de deux réseaux utilisant un système d'adressage nécessite deux piles réseau, (une pour chaque réseau).

Remarque : IBM Tealeaf Application de capture passive CX peut être configuré pour capturer les adresses IPv6 uniquement, les adresses IPv4 uniquement ou alors, des adresses IPv6 et IPv4 ou encore des adresses IPv6 avec IPv4 intégré.

Remarque : Les adresses IPv6 avec IPv4 intégré ne peuvent pas être insérées dans la console Web de la PCA mais vous pouvez insérer ces valeurs dans le fichier `ctc-conf.xml`. La PCA peut utiliser ces adresses. Voir «Méthodes de capture et de conversion d'adresses IP», à la page 292.

Voir Chapitre 1, «Présentation de Passive Capture», à la page 1.

Format IPv4

A l'origine, le protocole IP formatait les adresses IP comme illustré ci-dessous. Ce format était universel jusqu'à 2009.

```
AAA.BBB.CCC.DDD:EEEE
```

Dans l'exemple ci-dessus, chaque valeur constituée d'un ensemble de trois caractères est appelée octet.

- La valeur `EEEE` correspond à un numéro de port, elle est précédée de deux points (`:`).

Format IPv6

Une adresse IPv6 est représentée comme une séquence de huit groupes de quatre caractères hexadécimaux. Ces groupes sont séparés par deux points (`:`).

Le format IPv6 a été conçu pour succéder au format IPv4 puisqu'il fournit un éventail bien plus vaste d'adresses possibles. Le format IPv6 est bien plus présent sur Internet. Il est défini de la manière suivante :

```
2001:0db8:85a3:0000:0000:8a2e:0370:7334(8080)
```

Les caractères hexadécimaux ne sont pas sensibles à la casse mais doivent être représentés en minuscule par souci de cohérence.

Numéros de port

Comme la définition d'adresses a besoin de deux points (`:`) pour jouer le rôle de séparateur, ce caractère ne peut pas être utilisé comme marqueur du numéro de port comme dans l'adresse IPv4 :

```
https://langley:19000
```

L'utilisation de parenthèses est privilégiée, comme l'indique l'exemple suivant :

```
2001:0db8:85a3:0000:0000:8a2e:0370:7334(8080)
```

Remarque : Le numéro de port est entre parenthèses (8080). Pour les adresses IPv6, les recherches à partir du numéro de port ne sont pas prises en charge.

Simplifications

La représentation entière de huit groupes à quatre caractères peut être simplifiée à l'aide de plusieurs techniques permettant d'en éliminer certaines parties.

Zéros en début de groupe

Il est possible d'omettre les zéros qui se trouvent au début d'un groupe mais chaque groupe doit contenir au moins un caractère hexadécimal. L'exemple précédent pourrait être simplifié comme suit :

```
2001:db8:85a3:0:0:8a2e:370:7334
```

Remarquez la suppression de deux zéros en début de groupe et de deux ensembles d'octets composés de zéros.

Groupes de zéros

Un groupe de zéros ou plusieurs groupes successifs peuvent être remplacés par un seul groupe vide à l'aide de deux-points consécutifs (::).

- Cette substitution ne peut s'appliquer qu'une fois dans une adresse car plusieurs occurrences peuvent entraîner une représentation ambiguë.
- S'il est possible d'appliquer plusieurs substitutions, il faut alors utiliser la méthode qui permet de supprimer le plus de groupes. Si les deux méthodes permettent d'enlever le même nombre de groupes, il faut alors utiliser celle qui remplace les groupes les plus à gauche.

A l'aide de ces règles, l'adresse qui sert d'exemple peut être d'autant plus simplifiée :

```
2001:db8:85a3::8a2e:370:7334
```

Adresses spéciales

Tableau 23. Adresses spéciales

Nom de l'adresse	Adresse brute	Adresse réduite
Adresse du système hôte local (bouclage)	0:0:0:0:0:0:0:1	::1
Adresse IPv6 non définie	0:0:0:0:0:0:0:0	::

Source : http://www.wikipedia.org

Activation de la capture d'adresses IPv6

Pour plus d'information sur la manière d'activer la capture d'adresses IPv6 dans les builds 35xx et ultérieures de la PCA, contactez Tealeaf http://support.tealeaf.com.

Capture

Vous trouverez dans cette section des explications sur les méthodes permettant de capturer et de convertir les adresses IP ainsi que sur la prise en charge du protocole IPv6 par la PCA.

Méthodes de capture et de conversion d'adresses IP

Pour rendre les adresses IPv6 disponibles à la recherche, il faut capturer des adresses IPv4 ou des adresses IPv6. Ces adresses sont normalisées dans un format connu des processus d'indexation et de recherche de Tealeaf.

Tealeaf prend en charge deux méthodes de capture et de conversion d'adresses :

- PCA : lorsque la build 3501 ou ultérieure de la PCA est déployée, la capture d'adresses IPv6 peut être activée. Les adresses IPv4 peuvent être converties au format IPv6 pour les fonctions d'indexation et de recherche. Voir «Prise en charge du protocole IPv6 par la PCA».
- Agent de session de déploiement : s'il est impossible de mettre à niveau la PCA vers une version qui prend en charge le protocole IPv6, vous devez déployer l'agent de session de déploiement pour insérer les valeurs appropriées dans la demande pour indexer et rechercher les adresses IPv6. Voir section "Agent de session de déploiement" dans le manuel de configuration d'*IBM Tealeaf CX*.

  Remarque : Cette méthode est accessible dans les éditions 8.4 et ultérieures.

  Remarque : Si vous ne pouvez pas mettre à niveau votre PCA vers la build 3501 ou une version plus récente, vous devez déployer l'agent de session de déploiement dans chaque pipeline Windows qui effectue du traitement pour que l'indexation et la recherche d'adresses IPv6 soient possibles.

Prise en charge du protocole IPv6 par la PCA

A partir de la build 3501, IBM Tealeaf Application de capture passive CX peut être configuré afin de capturer des adresses IPv6. La PCA peut compresser ces adresses et activer la configuration à l'aide des adresses IPv6.

Remarque : Le protocole IPv6 ne peut pas être activé à l'aide de la console Web de la PCA. Pour plus d'informations, contactez Tealeaf http://support.tealeaf.com.

Voir section Comment la PCA gère-t-elle la capture des adresses IPv6.

Insertion de données dans la demande

L'insertion de données dans la demande implique un format IPv6 et un mode de conversion.

Format IPv6

Si la capture d'adresses IPv6 est activée et que des adresses IPv6 sont détectées dans le flux de capture, les variables suivantes sont insérées dans la section `[env]` de la demande :

```
[env]
...
IPV6_XLAT=False
IPV6=True
...
REMOTE_ADDR=fe80::20b:dbff:fe93:a462
LOCAL_ADDR=fe80::213:72ff:fe67:ed26
```

```
SERVER_NAME=fe80::213:72ff:fe67:ed26
IPV6_REMOTE_ADDR=FE80:0000:0000:0000:020B:DBFF:FE93:A462
IPV6_LOCAL_ADDR=FE80:0000:0000:0000:0213:72FF:FE67:ED26
IPV6_SERVER_NAME= fe80::213:72ff:fe67:ed26
...
```

Zone **Description**

IPV6_XLAT
Lorsque la variable IPv6 est paramétrée sur True, cette option indique, si elle est paramétrée sur True, si des adresses IP insérées dans la requête IPv4 doivent être converties.

IPV6 Indique si le trafic capturé est au format IPv6, si elle est paramétrée sur True.

REMOTE_ADDR
Affiche l'adresse IP brute, comme elle a été capturée, pour que l'adresse distante puisse être soit au format IPv6, soit au format IPv4.
- La PCA peut insérer cette valeur.

  Remarque : Cette valeur peut être compressée au format IPv6.

LOCAL_ADDR
Affiche l'adresse IP brute, comme elle a été capturée, pour que l'adresse locale puisse être soit au format IPv6, soit au format IPv4.
- La PCA peut insérer cette valeur.

  Remarque : Cette valeur peut être compressée au format IPv6.

SERVER_NAME
Le nom de zone existant peut maintenant accepter des données au format IPv6.

Remarque : SERVER_NAME n'est pas indexé.

IPV6_REMOTE_ADDR
Valeur REMOTE_ADDR rendue au format IPv6 non compressé
- La PCA peut insérer cette valeur.

IPV6_LOCAL_ADDR
La valeur LOCAL_ADDR rendue au format IPv6 non compressé
- La PCA peut insérer cette valeur.

IPV6_SERVER_NAME
Le nouveau nom de zone est utilisé pour stocker la valeur SERVER_NAME au format IPv6 non compressé.

Mode de conversion IPv6

Dans le mode de conversion IPv6, la PCA convertit des adresses qui étaient à l'origine au format IPv4 dans un format lisible à l'aide de composants des serveurs de Windows Tealeaf. La PCA insère dans la demande les zones suivantes. En plus des zones, elle insère les valeurs originales pour les variables suivantes :
- IPV6_REMOTE_ADDR_ORIG
- IPV6_LOCAL_ADDR_ORIG
- IPV6_SERVER_NAME_ORIG

Exemple :

```
IPV6_XLAT=True
IPV6=True
REMOTE_ADDR=254.147.164.98
LOCAL_ADDR=254.103.237.38
SERVER_NAME=254.103.237.38
?
IPV6_REMOTE_ADDR=0000:0000:0000:0000:0000:FFFF:FE93:A462
IPV6_LOCAL_ADDR=0000:0000:0000:0000:0000:FFFF:FE67:ED26
IPV6_SERVER_NAME=0000:0000:0000:0000:0000:FFFF:FE67:ED26
?
IPV6_REMOTE_ADDR_ORIG=FE80:0000:0000:0000:020B:DBFF:FE93:A462
IPV6_LOCAL_ADDR_ORIG=FE80:0000:0000:0000:0213:72FF:FE67:ED26
IPV6_SERVER_NAME_ORIG=FE80:0000:0000:0000:0213:72FF:FE67:ED26
```

Zone **Description**

IPV6_REMOTE_ADDR_ORIG
Contient l'adresse IPv6 originale pour l'option REMOTE_ADDR avant que celle-ci a été convertie.

IPV6_LOCAL_ADDR_ORIG
Contient l'adresse IPv6 originale pour l'option LOCAL_ADDR avant que celle-ci a été convertie.

IPV6_SERVER_NAME_ORIG
Contient l'adresse IPv6 d'origine pour l'option SERVER_NAME avant que celle-ci a été convertie.

Voir «Format IPv6», à la page 292.

Annexe F. Documentation et aide d'IBM Tealeaf

IBM Tealeaf fournit une documentation et une aide aux utilisateurs, développeurs et administrateurs.

Affichage de la documentation du produit

L'intégralité de la documentation des produits IBM Tealeaf est disponible sur le site Web suivant :

https://tealeaf.support.ibmcloud.com/

Utilisez les informations du tableau suivant pour afficher la documentation des produits d'IBM Tealeaf :

Tableau 24. Obtention de l'aide

Pour afficher...	Procédez comme suit...
Documentation du produit	Dans le portail IBM Tealeaf , accédez à **?** > **Documentation du produit**.
Aide d'une page sur le portail IBM Tealeaf	Dans le portail IBM Tealeaf , accédez à **?** > **Aide de cette page**.

Documents disponibles pour les produits IBM Tealeaf

Utilisez le tableau suivant pour afficher une liste des documents disponibles pour tous les produits IBM Tealeaf :

Tableau 25. Documentation disponible pour les produits IBM Tealeaf

Produits IBM Tealeaf	Documents disponibles
IBM Tealeaf CX	• *IBM Tealeaf Customer Experience - Guide de présentation* • *IBM Tealeaf CX Client Framework - Guide d'intégration des données* • *IBM Tealeaf CX - Guide de configuration* • *Guide d'IBM Tealeaf CX Cookie Injector* • *IBM Tealeaf CX - Guide des bases de données* • *Guide d'IBM Tealeaf CX Event Manager* • *IBM Tealeaf CX - Glossaire* • *IBM Tealeaf CX - Guide d'installation* • *Guide d'IBM Tealeaf CX PCA* • *IBM Tealeaf CX PCA - Notes sur l'édition*

Tableau 25. Documentation disponible pour les produits IBM Tealeaf (suite)

Produits IBM Tealeaf	Documents disponibles
IBM Tealeaf CX	• *Guide d'IBM Tealeaf CX RealiTea Viewer Client Side Capture* • *IBM Tealeaf CX RealiTea Viewer - Guide d'utilisation* • *IBM Tealeaf CX - Notes sur l'édition* • *IBM Tealeaf CX Release - Guide de mise à niveau* • *IBM Tealeaf CX Support - FAQ sur le traitement des incidents* • *IBM Tealeaf CX - Guide de traitement des incidents* • *Guide d'IBM Tealeaf CX UI Capture j2* • *IBM Tealeaf CX UI Capture j2 - Notes sur l'édition*
IBM Tealeaf cxImpact	• *IBM Tealeaf cxImpact - Guide d'administration* • *IBM Tealeaf cxImpact - Guide d'utilisation* • *IBM Tealeaf cxImpact - Guide de génération de rapports*
IBM Tealeaf cxConnect	• *IBM Tealeaf cxConnect for Data Analysis - Guide d'administration* • *IBM Tealeaf cxConnect for Voice of Customer - Guide d'administration* • *IBM Tealeaf cxConnect for Web Analytics - Guide d'administration*
IBM Tealeaf cxOverstat	*IBM Tealeaf cxOverstat - Guide d'utilisation*
IBM Tealeaf cxReveal	• *IBM Tealeaf cxReveal - Guide d'administration* • *IBM Tealeaf cxReveal - Guide de l'API* • *IBM Tealeaf cxReveal - Guide d'utilisation*
IBM Tealeaf cxVerify	*IBM Tealeaf cxVerify - Guide d'administration*
IBM Tealeaf cxView	*IBM Tealeaf cxView - Guide d'utilisation*
IBM Tealeaf CX Mobile	• *IBM Tealeaf CX Mobile Android Logging Framework Guide* • *IBM Tealeaf Android Logging Framework - Notes sur l'édition* • *IBM Tealeaf CX Mobile - Guide d'administration* • *IBM Tealeaf CX Mobile - Guide d'utilisation* • *Guide d'IBM Tealeaf CX Mobile iOS Logging Framework* • *IBM Tealeaf iOS Logging Framework - Notes sur l'édition*

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays.

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Contactez votre interlocuteur IBM local pour plus de détails sur les produits et les services actuellement disponibles dans votre pays. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet en cours couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous accorde aucun licence sur ces brevets. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.
Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7 Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japon

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales. LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Bay Area Lab
1001 E Hillsdale Boulevard
Foster City, California 94404
U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions du Contrat sur les produits et services IBM, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins

illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel contient des échantillons de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces échantillons de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmes d'application pour lesquels ils ont été écrits. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la serviçabilité ou le fonctionnement de ces programmes. Les exemples de programmes sont fournis "en l'état", sans garantie d'aucune sorte. IBM ne sera en aucun cas responsable des dommages liés à l'utilisation de ces programmes exemples.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. D'autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. Une liste de marques IBM est actuellement disponible sur Internet sur le site «Copyright and trademark information» à l'adresse www.ibm.com/legal/copytrade.shtml.

Remarques sur les règles de confidentialité

Les produits IBM Software, notamment les logiciels sous forme de services ("Offre logicielles") peuvent utiliser des cookies ou d'autres technologies pour collecter des informations d'utilisation en vue d'améliorer l'expérience de l'utilisateur final, d'ajuster les interactions avec l'utilisateur final ou à d'autres fins. Un cookie est une donnée qu'un site Web peut envoyer à votre navigateur et qui peut ensuite être stockée sur votre ordinateur sous la forme d'une balise identifiant ce dernier. Dans la plupart des cas, aucune information personnelle n'est collectée par ces cookies. Si vous utilisez une Offre logicielle qui vous permet de collecter des informations personnelles via des cookies et des technologies similaires, tenez compte des spécificités suivantes.

En fonction de la configuration déployée, cette Offre logicielle peut utiliser des cookies de session et des cookies permanents qui collectent le nom de chaque utilisateur, ainsi que d'autres informations personnelles à des fins de gestion des sessions, de convivialité améliorée pour l'utilisateur ou d'autres objectifs de suivi de l'utilisation ou fonctionnels. Ces cookies peuvent être désactivés mais leur désactivation élimine également la fonctionnalité qu'ils activent.

Diverses juridictions régulent la collecte d'informations personnelles via les cookies et autres technologies similaires. Si la configuration déployée pour cette Offre logicielle vous permet, en tant que client, de collecter des informations personnelles d'utilisateurs finaux via des cookies et autres technologies, vous devez rechercher votre propre avis légal concernant les lois applicables à cette collecte de données, dont toutes les exigences de mention et d'accord, le cas échéant.

IBM exige que les Clients (1) fournissent un lien clair et visible vers les conditions d'utilisation du site Web du client (par exemple, les règles de confidentialité), avec

un lien vers les collectes de données et les pratiques d'utilisation d'IBM et du Client, (2) indiquent que des cookies et des alarmes Web/gifs invisibles sont placés sur l'ordinateur du visiteur par IBM pour le compte du Client, en expliquant l'objectif de cette technologie et (3) selon les conditions requises par la loi, obtiennent le consentement des visiteurs du site Web avant de placer les cookies et les alarmes Web/gifs par le Client ou IBM sur leurs unités.

Pour plus d'informations sur l'utilisation des diverses technologies, notamment des cookies, reportez-vous à la section intitulée Cookies, Web Beacons and Other Technologies d'IBM à l'adresse http://www.ibm.com/privacy/details/us/en.

IBM®